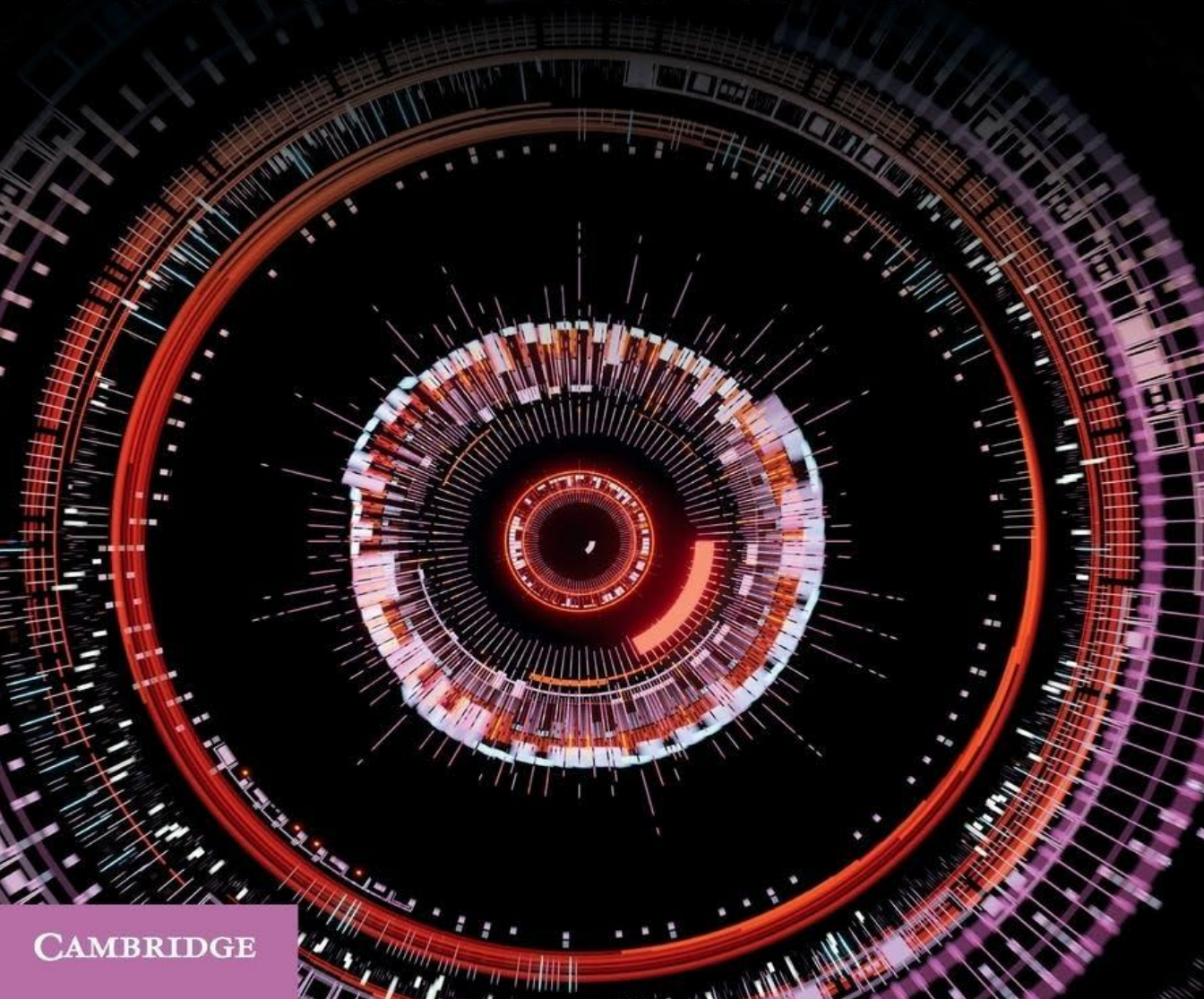


The Cambridge Handbook of **DIGITAL EVIDENCE IN CRIMINAL INVESTIGATIONS**

EDITED BY

Vanessa Franssen and Stanisław Tosza



CAMBRIDGE



INVESTIGADOR_Z

INVESTIGADOR_Z

THE CAMBRIDGE HANDBOOK OF DIGITAL EVIDENCE IN CRIMINAL INVESTIGATIONS

Authored by leading scholars in the field, this handbook delves into the intricate matter of digital evidence collection, adopting a comparative and intradisciplinary approach. It focuses specifically on the increasingly important role of online service providers in criminal investigations, which marks a new paradigm in the field of criminal law and criminal procedure, raising particular challenges and fundamental questions. This scholarly work facilitates a nuanced understanding of the multifaceted and cross-cutting challenges inherent in the collection of digital evidence, as it navigates the contours of current and future solutions against the backdrop of ongoing European and international policy-making. As such, it constitutes an indispensable resource for scholars and practitioners alike, offering invaluable insights into the evolving landscape of digital evidence gathering.

Vanessa Franssen is a professor at the University of Liège where she teaches criminal law, national and comparative criminal procedure, as well as cybercrime. Her current research centers on the impact of new technologies on criminal justice, at both national and European levels. Furthermore, she has extensive research experience in the field of European Union and comparative criminal law and procedure, economic criminal law as well as the interplay between criminal law and punitive administrative law.

Stanisław Tosza is Associate Professor in Compliance and Law Enforcement at the University of Luxembourg, where he researches and teaches comparative and European criminal law and criminal procedure, white-collar crime, cybercrime and cyberlaw. In his research he focuses in particular on the role of private actors in enforcement as well as the challenges of new technologies for criminal justice. He is the Secretary General of the International Association of Penal Law (AIDP).

The Cambridge Handbook of Digital Evidence in Criminal Investigations

Edited by

VANESSA FRANSSEN

University of Liège

STANISŁAW TOSZA

University of Luxembourg



INVESTIGADOR_Z



Shaftesbury Road, Cambridge CB2 8EA, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre,
New Delhi – 110025, India

103 Penang Road, #05–06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of Cambridge University Press & Assessment,
a department of the University of Cambridge.

We share the University's mission to contribute to society through the pursuit of
education, learning and research at the highest international levels of excellence.

www.cambridge.org

Information on this title: www.cambridge.org/9781316511275

DOI: [10.1017/9781009049771](https://doi.org/10.1017/9781009049771)

© Cambridge University Press & Assessment 2025

This publication is in copyright. Subject to statutory exception and to the provisions
of relevant collective licensing agreements, no reproduction of any part may take
place without the written permission of Cambridge University Press & Assessment.

When citing this work, please include a reference to the DOI [10.1017/9781009049771](https://doi.org/10.1017/9781009049771)

First published 2025

A catalogue record for this publication is available from the British Library

A Cataloging-in-Publication data record for this book is available from the Library of Congress

ISBN 978-1-316-51127-5 Hardback

Cambridge University Press & Assessment has no responsibility for the persistence
or accuracy of URLs for external or third-party internet websites referred to in this
publication and does not guarantee that any content on such websites is, or will remain,
accurate or appropriate.

Contents

<i>List of Tables</i>	<i>page</i> viii
<i>List of Contributors</i>	ix
<i>Foreword</i>	
John Vervaele	xi
Introduction: Gathering Electronic Evidence and Cooperation with Service Providers in the Digital Era – A Jigsaw Puzzle of Technological and Legal Challenges	1
Vanessa Franssen and Stanisław Tosza	
PART I COLLECTING DIGITAL EVIDENCE: TRANSVERSAL CHALLENGES AND SOLUTIONS	11
1 Impact of Digital Evidence Gathering on the Criminal Justice System: A Broader Perspective	13
Anže Erbežnik	
2 Unresolved Jurisdictional Issues in Law Enforcement Access to Data	43
Dan Svantesson and Anna-Maria Osula	
3 Effective Data Protection and Direct Cooperation on Digital Evidence	68
Gavin Robinson	
4 On Encryption Technologies and Potential Solutions for Lawful Access	104
Cyprien Delpéch de Saint Guilhem	
5 Admissibility of Digital Evidence	126
Giulia Lasagni	
6 Exchange of Data between National Security Agencies and Law Enforcement: Challenges for Criminal Procedure	153
Tatiana Tropina	
7 From Mutual Trust to the Gordian Knot of Notifications: The EU e-Evidence Regulation and Directive	173
Theodore Christakis	

8	Moving in the Right Direction for Transborder Access to Digital Evidence in Criminal Matters? The Council of Europe and the Second Additional Protocol Introducing Direct Cooperation Mechanisms	200
	Ma. Angela Leonor Aguinaldo and Paul de Hert	
	PART II DIGITAL EVIDENCE AND THE COOPERATION OF SERVICE PROVIDERS IN EU CRIMINAL INVESTIGATIONS	219
9	Digital Evidence in Criminal Matters: Belgian Pride and Prejudice	221
	Sem Careel and Frank Verbruggen	
10	Digital Evidence in Estonia	261
	Agnes Kasper, Eneli Laurits and Melita Sogomonjan	
11	Digital Evidence and the Cooperation of Service Providers in Germany	289
	Dominik Brodowski	
12	Accessing Digital Evidence in Criminal Matters: An Inadequate Irish Legal Framework	309
	T. J. McIntyre and Maria Helen Murphy	
13	Digital Evidence and the Cooperation of Service Providers in Luxembourg	347
	Katalin Ligeti and Gavin Robinson	
14	Gathering of Digital Evidence and Cooperation of Service Providers in Poland	374
	Maciej Rogalski	
15	Access to Retained Data and Cooperation of Service Providers in Criminal Investigations in Spain	400
	Carmen Cuadrado Salinas and Juan Carlos Ortiz Pradillo	
16	A Comparative Analysis of National Law and Practices: Unravelling Differences in View of EU-Wide Solutions	423
	Stanisław Tosza and Vanessa Franssen	
	PART III COLLECTING DIGITAL EVIDENCE AND THE ROLE OF SERVICE PROVIDERS: A GLOBAL PERSPECTIVE	455
17	Digital Evidence and Cooperation of Service Providers in China	457
	Li Zhe and Jin Zhenan	
18	Cooperation of Service Providers in Criminal Investigations in the Russian Federation	486
	Maria Filatova, Olga Kostyleva and Tatiana Alekseeva	
19	Digital Evidence Collection in Turkey	512
	Seçil Bilgiç	
20	Obtaining Digital Evidence under UK Law	539
	Elif Mendos Kuşkonmaz and Ian Walden	

21	Digital Evidence Gathering by US Authorities and Cross-Border Cooperation with US-Based Service Providers	569
	Marine Corhay and Vanessa Franssen	
	Conclusion: Collecting Digital Evidence – From Present Challenges to Future Solutions	587
	Vanessa Franssen and Stanisław Tosza	

Tables

9.1	Overview of cooperation duties	<i>page</i> 238
10.1	Data collection authorisations in investigations	265
12.1	Summary of data access methods under Irish law	327
18.1	Examples of data retention obligations	489
18.2	Types of liability for violations of data subjects' rights	493
19.1	Total number of reported section 10 offences over the years	515

Contributors

Ma. Angela Leonor Aguinaldo, Associate Professorial Lecturer, De La Salle University, Philippines.

Tatiana Alekseeva, PhD student, Law Faculty, Moscow State University and lawyer at the Analytical Center of Criminal Law and Criminology, LLC, Russia.

Seçil Bilgiç, LLM Harvard Law School (Fulbright Scholar); technology transactions lawyer at Cohesity; admitted to the New York State Bar and the Istanbul Bar Association; formerly mergers and acquisitions/corporate lawyer at White & Case LLP.

Dominik Brodowski, Professor of Europeanization, Internationalization and Digital Transformation of Criminal Law and Criminal Procedure, Saarland University, Germany.

Sem Careel, FWO PhD researcher, Institute of Criminal Law, KU Leuven, Belgium.

Theodore Christakis, Professor of International, European and Digital Law at Grenoble Alps University, France and Director of Research for Europe with the Cross-Border Data Forum.

Marine Corhay, PhD candidate (FRESH grantee) FRS-FNRS, University of Liège, Belgium.

Carmen Cuadrado Salinas, Senior Lecturer in Criminal Procedure Law, Fellow at Faculty of Law, University of Alicante, Spain.

Paul de Hert, Professor of Law, Faculty of Law and Criminology, Free University of Brussels, Belgium and Associate Professor of Law and Technology, Tilburg Institute for Law and Technology (TILT), The Netherlands.

Cyprien Delpech de Saint Guilhem, FWO Postdoctoral Fellow, Computer Security and Industrial Cryptography (COSIC), KU Leuven, Belgium.

Anže Erbežnik, Professor of Criminal Law and Criminal Procedure, European Law Faculty, Slovenia and Advisor in the Secretariat of the European Parliament's Legal Affairs Committee and before of its Justice, Home Affairs and Fundamental Rights Committee.

Maria Filatova, PhD, Head of the Analytical Center of Criminal Law and Criminology, Russia.

Vanessa Franssen, Professor of Criminal Law and Criminal Procedure, University of Liège and Affiliated Senior Researcher, Institute of Criminal Law, KU Leuven, Belgium.

Agnes Kasper, PhD, Senior Lecturer of Technology Law, Tallinn University of Technology, Estonia.

Olga Kostyleva, Assistant Professor, Law Faculty, Moscow State University, Russia.

Elif Mendos Kuşkonmaz, Lecturer in Law, University of Essex, United Kingdom.

Giulia Lasagni, Senior Assistant Professor in Criminal Procedure, University of Bologna, Italy.

Eneli Laurits, State Prosecutor dealing with corruption-related crimes, Estonia.

Katalin Ligeti, Professor of European and International Criminal Law and Dean of the Faculty of Law, Economics and Finance, University of Luxembourg; President of the International Association of Penal Law.

T. J. McIntyre, Associate Professor, University College Dublin Sutherland School of Law and Chairperson of Digital Rights Ireland.

Maria Helen Murphy, Associate Professor, Maynooth University School of Law and Criminology, Ireland.

Juan Carlos Ortiz Pradillo, Professor of Civil and Criminal Procedure, Complutense University of Madrid, Spain.

Anna-Maria Osula, Senior Researcher, Tallinn University of Technology, Estonia and Research Fellow, Masaryk University, Czech Republic.

Gavin Robinson, Assistant Professor, eLaw – Center for Law and Digital Technologies, Leiden University, Netherlands.

Maciej Rogalski, Professor, Department of Criminal Law, Lazarski University and Rector of that university, Poland.

Melita Sogomonjan, Lecturer, Tallinn University of Technology, Estonia.

Dan Svantesson, Professor, Faculty of Law, Co-director for the Centre for Space, Cyberspace and Data Law, Bond University, Australia; Senior Fellow, Social Cyber Institute; Research Fellow, Masaryk University, Czech Republic; and Associated Researcher, Swedish Law and Informatics Research Institute, Stockholm University, Sweden.

Stanisław Tosza, Associate Professor in Compliance and Law Enforcement, University of Luxembourg and Secretary General of the International Association of Penal Law.

Tatiana Tropina, former Assistant Professor in Cybersecurity Governance, Institute of Security and Global Affairs at Leiden University, Netherlands.

Frank Verbruggen, Professor of Belgian, European and International Criminal Law, Institute of Criminal Law, KU Leuven, Belgium.

Ian Walden, Professor of Information and Communications Law, Centre for Commercial Law Studies, Queen Mary University of London, United Kingdom.

Li Zhe, Associate Professor, Faculty of Law, University of Macau.

Jin Zhenan, PhD candidate, Faculty of Law, University of Macau.

Foreword

Our digital information society comes with many advantages that will further increase with artificial intelligence (AI) applications. The digitalized world, be it in the area of communications, the Internet of Things or platform economies, not only produces and processes an enormous amount of data but also creates, through interconnectivity, new data knowledge and related applications. This bright side of innovative technologies, however, also comes with a dark side. Our daily digital fingerprint, based on location data and other, meta data, creates the possibility to construct a full personal digital identity. Data knowledge can be abused for preventive surveillance by states and companies, and undermine fundamental rights and democratic values.

The digital society is also an environment in which crime patterns change. New digital crimes are emerging and digital tools are meanwhile being used for committing common offenses of all types. The result is that access to electronic data for evidence purposes, commonly called digital or electronic evidence, has become indispensable in the large majority of criminal investigations. In the 2022 Sirius EU Digital Evidence Situation Report by Eurojust and Europol, we can read to what extent the request from law enforcement and judicial authorities to internet service providers (ISPs) has exploded and become a decisive tool in criminal investigations (Europol, “SIRIUS EU Digital Evidence Situation Report,” 4th Annual Report, 2022, p. 16). With the rapid advancement of AI technologies, the need for direct enforcement cooperation with ISPs and other private partners in the digital markets will only increase.

At the national level many states have adapted their criminal substantive law by introducing new cybercrimes and have revised their criminal procedural law by providing new tools for digital investigations, including production orders to ISPs located in their territory. The problem is, however, that the large majority of the ISPs are not established in the jurisdiction of the state of investigation or do not even offer services in that state, that the relevant data are located in multiple jurisdictions or that it is even unclear where they might be located. This globalization of digital criminal evidence leads to a disconnect with the territorial criminal jurisdiction of states and creates very significant obstacles for law enforcement agencies. As we all know, criminal law enforcement is strictly related to state sovereignty and territoriality, meaning that law enforcement agencies are not allowed to extend their operational investigative powers beyond their national borders. If they need transborder access to (digital) evidence, they have to rely on existing instruments of mutual legal assistance (MLA), which can be bilateral, multilateral or included in international repression conventions such as, for instance, the UN Convention on Transnational Crime (UNCTOC), the UN Convention on Corruption (UNCTAC) or the Council of Europe Convention on Cybercrime (Budapest Convention).

The problem with these conventions is that they rely on interstate cooperation and interstate requests between central authorities at the ministerial level. Most of these conventions have not been designed for digital evidence that is moreover mostly not in the hands of state authorities but held by the real gatekeepers in today's digital society: the ISPs. These conventions are also cumbersome, time-consuming and thus not really adapted to volatile digital information. However, these conventions contain standardized rules for cooperation and also provide for some minimum rights and remedies for the persons concerned.

In the light of this new reality and given the enforcement gap and the risk of impunity, national authorities have been experimenting with and attempting to regulate forms of cross-border access to data, outside of the existing MLA box. Legislators have come up with concepts such as the obligation for ISPs to locate data in the national jurisdiction or forms of extraterritorial investigative jurisdiction for serious crimes in exceptional circumstances, for instance when the digital evidence in point cannot be obtained on the basis of MLA. For their part, the law enforcement agencies have elaborated, based on national law, models of cooperation with ISPs on a voluntary basis, or have issued unilateral subpoenas for the production of data by foreign ISPs, or have used remote search and seizure (including so-called governmental hacking) in foreign jurisdictions or in cyberspace, in some cases in a legal limbo. This national unilateralism comes, of course, with tensions and clashes between states as well as between states and ISPs, but also triggers important questions in relation to sovereignty, international law standards, concepts of jurisdiction, the protection of fundamental rights and even data security. International law, unfortunately, also does not offer us any clear answers to the question whether these cross-border criminal investigative techniques could constitute a violation of sovereignty.

The demand for new regulatory standards is high and the international communities have been trying to come up with a new legal framework for the cross-border gathering of digital evidence in criminal matters. At the level of the Council of Europe, negotiations were launched in 2017 to elaborate a Second Additional Protocol to the Budapest Cybercrime Convention to enhance cooperation and the disclosure of electronic evidence. Although this is a regional Convention, it is the most important multilateral convention and the international standard in the field, as it has been ratified by important nonmember states of the Council of Europe and has also been a model for many national legislators, even in countries that have not joined the Convention. The negotiations on the Second Additional Protocol to the Cybercrime Convention were very difficult and intensive (more than ninety meetings), but were eventually concluded in 2022 and the Second Additional Protocol has been tabled for signature from May 12, 2022 onwards. Only parties to the main Convention are allowed to join. The Protocol contains, *inter alia*, an “emergency” MLA procedure in the case of a significant and imminent risk to the life or safety of any natural person and direct cooperation with ISPs, but this is limited to less intrusive data such as domain name registration or subscriber information. This means that content data, also very important for law enforcement, are excluded from direct cooperation with the ISPs. Clearly, the second Protocol did not bring about a convincing solution and is certainly not a game changer.

At EU level, the European Commission submitted, for its part, an e-evidence package in April 2018, as part of its broader regulatory Digital Agenda (Digital Markets Act, Digital Services Act, EU Data Act, Data Governance Act, AI Act, EU Media Freedom Act), its Security Strategy and its Priorities for the Area of Freedom, Security and Justice. The package contained a proposal for a directive and a proposal for a regulation. The directive provides for the obligation for ISPs active in the internal EU market to designate a legal representative in the EU. The regulation creates a European preservation order and a European production order, based on

mutual recognition, that a competent judicial authority can directly impose on foreign ISPs, thereby bypassing, to a large extent, the classic mutual recognition between the judicial authorities of the member states. Unlike the Second Additional Protocol to the Budapest Convention, this proposal consists of a real paradigm change as it invests the ISPs with a public role: it puts them in the position of an extended arm of the judicial authorities and also delegates the fundamental rights compliance check in the executing state largely to them. The negotiations on the EU e-evidence package were very intensive and difficult, as there were many disagreements between the member states and also between the European Commission, the Council of the EU and the European Parliament. The disagreements related, *inter alia*, to the bypassing of the judicial authorities of the executing state, the duties of the ISPs to check compliance with fundamental rights, the broad range of offenses, the types of data that should be covered, the grounds for refusal and the enforcement regime in the case of noncompliance by the ISPs.

Both the Regulation and the Directive were adopted in July 2023 and it seems that the model of direct cooperation with the ISPs has survived. The ISPs will be embedded in an EU-wide platform to guarantee the authenticity of the orders and the security of communications. The rights of ISPs to refuse cooperation are limited and ISPs are in principle obliged to produce the required data. Enforcement procedures and potentially significant sanctions (going up to 2 percent of the total worldwide annual turnover) shall assure compliance with the orders. Contrary to the Second Protocol, the e-evidence package has greater chances to become a real game changer introducing a completely new paradigm of public–private cooperation in the cross-border gathering of digital evidence in criminal matters.

Relevant is also the United States’ dimension where many important ISPs are established. In 2018, US Congress passed the CLOUD Act, under which ISPs can lift blocking provisions and produce data, including content data, related to non-US citizens and residents to foreign judicial authorities only if there is an executive agreement between the US and the country of the foreign judicial authority. Such agreement would allow for direct cooperation with the ISPs, even for content data, without channeling the judicial request through the MLA mechanisms. The first CLOUD Act executive agreement was concluded between the US and the UK in 2019, and entered into force on October 3, 2022. In the meantime, an agreement with Australia has been signed and negotiations with Canada have started. Negotiations between the US and the EU have also been launched, but have been stalled as they awaited the approval of the e-evidence package in the EU, and were revived once the agreement on the package was reached.

It is against the backdrop of all these challenges and legal developments that this Handbook comes in and is filling a real gap by giving us an insight into: (1) the phenomenon of digital evidence in criminal matters and the new challenges it creates, be they legal or technological; (2) the discussions at the scholarly and policy levels on relevant concepts and definitions; (3) the new legal instruments elaborated by the EU, the Council of Europe – including the issues that were discussed (heavily) around the negotiation table – and the US CLOUD Act; and (4) how national jurisdictions are (or will be) dealing with the challenges. As you will understand from these four dimensions, this Handbook offers a highly interesting and very valuable analysis of the state-of-the-art and the challenges to be overcome, from the point of view of both effective law enforcement and compliance with fundamental rights. The Handbook is based on an international and comparative research project directed by the two editors. They have in my opinion decided on a convincing structure for this Handbook, starting with Part I on “Collecting Digital Evidence: Transversal Challenges and Solutions.” In this first part the contributions not only set

the scene (the phenomenon, the impact of digitalization on criminal justice and so on) but also deal with the problem of definitions of digital evidence and the types of data, with unsolved problems of jurisdiction, digital investigative measures, digital evidence law as well as encryption technology and criminal justice. The contributions have been written not only by criminal lawyers but also by international public lawyers and computer scientists. In this part we also get an in-depth analysis of the new European and international legal framework for direct cooperation with ISPs when it comes to the gathering of digital information for evidence purposes in criminal matters.

Even when new international and European standards are of the utmost importance for judicial cooperation, the national regulations on the gathering and use of digital evidence are and will to a large extent remain the backbone for the law enforcement agencies. Therefore, the editors have made a very wise choice to include in this Handbook a substantial part on comparative criminal justice both in Europe (Part II) and worldwide (Part III), based on a convincing set of jurisdictions for a functional comparison and making use of a modeled questionnaire for the exercise. The richness of the comparative approach is threefold. First, it shows to which extent the national legislator and the judiciary (including in many cases constitutional courts) have been struggling with giving content to the new challenges in this field. Second, it also demonstrates the regulatory gaps in many countries. Third, it shows very clearly that exercising enforcement jurisdiction, particularly investigative jurisdiction, outside the national territory, based on a unilateral approach encounters quite some difficulties in law and in practice, from the point of view of both effective enforcement as well as compliance with fundamental rights. And thus the need for international standards is also based on evidence that is delivered by this national comparative analysis.

The Handbook clearly underpins the need for new legislative solutions at the international level in order to provide for effective enforcement. However, it also stresses that the game changer, by including the ISPs in the cooperation mechanisms, cannot come with a substantial loss of procedural safeguards and fundamental rights. Outsourcing fundamental rights compliance to ISPs is also outsourcing a positive obligation of states toward a private party and entails the risk of the privatization of enforcement and of human rights compliance. Finally, both the Council of Europe and the EU are international communities in which the rule of law and fundamental rights are key values. If they want to be global trendsetters, they will have to find a convincing balance between the interest of effective criminal enforcement and the protection of fundamental rights. If the security approach were to become the leading factor in the new cooperation instruments, then these instruments would risk undermining the key values not only of the criminal justice systems but also of the international communities in which they are adopted.

Prof. Dr. John A. E. Vervaele
*Professor at the College of Europe, Bruges; Emeritus Professor
of Economic and European Criminal Law, Utrecht University,
Honorary President of the International Association
of Penal Law (AIDP-IAPL)*

Introduction

Gathering Electronic Evidence and Cooperation with Service Providers in the Digital Era – A Jigsaw Puzzle of Technological and Legal Challenges

Vanessa Franssen and Stanisław Tosza

TECHNOLOGICAL AND LEGAL CHALLENGES TO COLLECTING DIGITAL EVIDENCE

Over the last couple of decades, information and communications technologies (ICTs) have thoroughly reshaped the way in which people communicate with each other and the way in which they store, access and share information. Information is no longer stored (only) locally on a device but is retained in the cloud; it is shared in ways that were unthinkable for those who grew up before the start of the new millennium. These ICTs have made communication so much easier and faster, from almost anywhere in the world. Moreover, many of these technologies are now at the reach of all, and at low cost. The increased digitalisation of everyday life has many advantages and is thus often considered a positive evolution. Yet, the wide use of such technologies also creates unprecedented risks, which are eagerly exploited by criminals.

For law enforcement authorities (LEAs),¹ those technologies present numerous challenges when fighting crime today. In nearly every criminal investigation, LEAs are confronted with perpetrators and/or victims who used an electronic device and/or communicated in some way through the internet (via email, voice over internet protocol (VoIP) or internet telephony, chat sessions or online games, private messaging applications or social media). This holds true not only for typical ‘target cybercrimes’ (e.g., hacking) and ‘content-related cybercrimes’ (e.g., the distribution of child sexual abuse material or online hate speech) but also for ordinary offences (such as fraud, organised crime, drug trafficking and terrorism) when committed by means of a computer or information system (i.e., cyber-enabled crimes), leaving precious digital traces that could be used as evidence. Therefore, the need to gather digital or electronic² evidence – for both inculpatory and exculpatory purposes – is high.

Yet, while the need for collecting such data in the context of concrete criminal investigations (as opposed to bulk collection of data for national security purposes, raising different, though related questions) is beyond doubt, LEAs face multiple hurdles when it comes to collecting digital evidence. First, the existing investigative tools and powers they have do not always square with the new technological reality. Second, data is inherently volatile, for both technological and legal reasons, and its location of storage is often uncertain or changing due to the characteristics of the data infrastructure. Third, to protect the data and the privacy of their users, companies providing

¹ The term ‘law enforcement authorities’ is used in this book as a short-hand for ‘police and judicial authorities’, that is, all competent authorities that intervene in the detection, investigation and prosecution of criminal offences. It excludes intelligence or national security agencies.

² In this volume both terms are used interchangeably.

such technologies are applying increasingly stronger security-enhancing techniques. Users, too, commonly use encryption software to protect the content of their data and have good (or bad) reasons to avoid disclosing their location and identity to others (e.g., by using a proxy server or onion routing software like Tor). However, the use of encryption and anonymised communication networks obviously complicates the conduct of criminal investigations.

Due to the technological reality, evidence gathering relies increasingly on the cooperation of private actors, mostly ICT companies or providers of online or ‘network-based’³ services (in short: service providers). Without their help, LEAs would simply not be able to detect, investigate and/or prosecute a growing number of offences.⁴ Indeed, without their cooperation, many criminal investigations would be, if not impossible, at least much more cumbersome or, worse, would depend on evermore intrusive investigative measures and techniques, such as governmental ‘hacking’, an obligation for service providers to create so-called backdoors (see the legal battle between the FBI and Apple regarding iPhone security settings in the San Bernardino terrorist attack)⁵ and the use of surveillance spyware by LEAs.⁶ Such measures not only severely impact the fundamental rights of the individual suspects concerned but also affect the security of all users of the same technology or service.⁷

Cooperation between LEAs and private actors is, of course, nothing new – LEAs have been collaborating for several decades with telecommunications operators and providers as well as with financial institutions – but this cooperation has become increasingly challenging as new technologies and online services emerge and many of them are provided by global service providers located outside the territory of the investigating LEAs, operating under different legal regimes. When a service provider is located in another country, or when the data is stored abroad, LEAs should in principle resort to mutual legal assistance (MLA) because their coercive powers are limited to their national territory. The MLA rules are designed to facilitate judicial cooperation between states to gather or exchange information for law enforcement purposes. However, MLA procedures, which have been conceived in such a way as to make sure that the sovereignty of other states is duly respected,⁸ are burdensome and slow.⁹ While several efforts have been made to speed up MLA procedures, they remain a real problem for LEAs.¹⁰

³ This term is used by the EU legislator in the recently adopted e-Evidence Regulation. See Regulation (EU) 2023/154 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191/118 (e-Evidence Regulation), Recital (7).

⁴ See, e.g., S. Tosza, ‘Internet Service Providers as Law Enforcers and Adjudicators: A Public Role of Private Actors’ (2021) 43 *Computer Law & Security Review* 1.

⁵ See, e.g., C. Liguori, ‘Exploring Lawful Hacking as a Possible Answer to the “Going Dark” Debate’ (2020) 26 *Michigan Telecommunications and Technology Law Review* 317, 323–325.

⁶ See, e.g., European Parliament, Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware, *Report of the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware* (2023/2500(RSP)), B9-0260/2023, 22 May 2023, paras. 72–79, www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html.

⁷ On countering the exploitation of vulnerabilities, see, e.g., European Parliament, *Draft Recommendation to the Council and the Commission pursuant to Rule 208(12) of the Rules of Procedure following the Investigation of Alleged Contraventions and Maladministration in the Application of Union Law in Relation to the Use of Pegasus and Equivalent Surveillance Spyware* (2023/2500(RSP)), B9-0260/2023, 22 May 2023, paras. 72–79, www.europarl.europa.eu/doceo/document/B-9-2023-0260_EN.html.

⁸ See M. Giacometti, *La récolte transfrontière de preuves électroniques dans le contexte européen* (Brussels: Bruylant/Larcier, 2023), 141, para. 200.

⁹ For a further analysis of the shortcomings of MLA procedures, see S. Tosza, ‘Gathering Cross-Border Digital Evidence: Mutual Legal Assistance, Its Shortcomings and Remedies’, in V. Franssen and D. Flore (eds.), *Société numérique et droit pénal: Belgique, France, Europe* (Brussels: Bruylant, 2019), 271–273.

¹⁰ See, e.g., Europol, *SIRIUS EU Digital Evidence Situation Report*, 4th Annual Report (The Hague: European Union Agency for Law Enforcement Cooperation (Europol), 2022), 19 and 23, www.europol.europa.eu/cms/sites/default/

In reaction to this problem and the need for digital evidence, there has been a shift in recent years to more and more direct cooperation with foreign service providers. This ‘new paradigm’¹¹ has been fiercely criticised,¹² but nevertheless is part of LEAs’ daily practices in many countries. This cooperation sometimes takes place on a voluntary basis, without a clear legal basis, and the extent of such informal cooperation remains unclear, raising great concerns of accountability, legal certainty and the protection of fundamental rights. Very often, however, the cooperation between service providers and LEAs is considered compulsory, based on formal cooperation rules under national criminal procedure. These cooperation rules are challenged by fast technological (and economic) developments, challenges that become particularly tangible when considering the personal, material and territorial scope of application of those rules. For instance, it is not always clear which (kinds of) service providers are covered by such duties. The same holds true for the types of data: data categorisations may differ across fields of law (e.g., criminal procedure and data protection law) and may also evolve over time. Moreover, the enforceability of such cooperation duties to service providers established abroad is questionable.¹³ In addition to the problems related to the scope of national rules, the cooperation duties of service providers also vary considerably from one country to another.

Consequently, service providers operating in various legal systems are subject to different legal frameworks and requirements – a situation that inevitably results in conflicting legal obligations. Such conflicts lead to legal uncertainty and are likely to hamper the freedom to conduct business (Art. 16 of the Charter of Fundamental Rights of the EU). Furthermore, at a global level, the cooperation of service providers risks falling prey to non-democratic regimes and could seriously endanger the human rights of political opponents, journalists, minorities and so on.

Finally, citizens (or ‘data subjects’ as they are called in data protection law) find themselves in a particularly delicate situation as it has become difficult to foresee which legislation they will be subject to, which authorities and private actors have access to their data and which legal safeguards they are entitled to. At the international level, legislation and case law are extremely scattered and hardly contribute to the desperately needed legal certainty for citizens living in a strongly interconnected and globalised world.

At EU level, this scattered national approach has been considered a major concern for several reasons. Taking the perspective of LEAs, the Council of the EU stressed the importance of digital evidence in its conclusions of 9 June 2016 and identified the lack of a common EU

[files/documents/SIRIUS_DESR_2022.pdf](#), discussing the issues encountered by EU law enforcement authorities when requesting cross-border access to electronic evidence to both EU member states and third states.

¹¹ M. Corhay, ‘Private Life, Personal Data Protection and the Role of Service Providers: The EU e-Evidence Proposal’ (2021) 6(1) *European Papers* 442; V. Mitsilegas, ‘The Privatization of Mutual Trust in Europe’s Area of Criminal Justice: The Case of e-Evidence’ (2018) 25(3) *Maastricht Journal of European and Comparative Law* 264. Compare with V. Franssen, ‘Droit pénal et numérique: Vers un nouveau paradigme?’ (2018) 1 *Revue de la faculté de droit de l’Université de Liège* 195–203; Tosza, ‘Internet Service Providers as Law Enforcers and Adjudicators’, 2 and 12.

¹² See, e.g., E. Sellier and A. Weyembergh, *Criminal Procedural Laws Across the European Union – A Comparative Analysis of Selected Main Differences and the Impact They Have over the Development of EU Legislation*, Study commissioned by the LIBE Committee of the European Parliament (2018), www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/10-10/IPOL_STU2018604977_EN.pdf; M. Böse, *An Assessment of the Commission’s Proposals on Electronic Evidence*, Study commissioned by the LIBE Committee of the European Parliament (2018), [www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU\(2018\)604989_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf); S. Carrera, M. Stefan and V. Mitsilegas, *Cross-Border Data Access in Criminal Proceedings and the Future of Digital Justice: Navigating the Current Legal Framework, and Exploring Ways Forward Within the EU and Across the Atlantic*, Report of a CEPS and QMUL [Queen Mary University of London] task force (Brussels: Centre for European Policy Studies (CEPS), 2020).

¹³ See, e.g., K. De Schepper and F. Verbruggen, ‘Ontsnappen space invaders aan onze pacmannen? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners’ (2013) 3 *Tijdschrift voor Strafrecht* 153. For further analysis, see Chapter 16 in this volume.

framework on cross-border cooperation with service providers as an impediment to effective criminal investigations.¹⁴ For this reason, it called upon the European Commission to prepare a legal initiative on a common EU legal framework, ensuring effective criminal investigations and due respect for fundamental rights. Looking at the situation from a different perspective, the fragmented legal framework also hampers the proper functioning of the EU internal market and the development of the Digital Single Market. For this reason, too, it was desirable to create a level playing field for online service providers in the EU and to clarify their obligations to cooperate with LEAs, not just when they participate in the collection of digital evidence but also with respect to the illegal online content they host.¹⁵ Considering this crucial role of service providers and the complications resulting from their role in enforcement in cyberspace, this handbook on digital evidence puts them at the heart of the analysis, dedicating special attention to cooperation mechanisms provided for at national, supranational and international levels.

LEGAL FRAMEWORK ON GATHERING DIGITAL EVIDENCE AND COOPERATION WITH SERVICE PROVIDERS

Whereas the international legal framework was rather limited in 2015 when the editors of this handbook started researching the topic of digital evidence gathering, with some relevant legal provisions in the 2001 Cybercrime Convention of the Council of Europe¹⁶ and a patchwork of (mostly bilateral) MLA treaties, the legal landscape looks quite different today.¹⁷ A Second Additional Protocol to the Cybercrime Convention was agreed upon in November 2021,¹⁸ after four years of difficult negotiations, and will soon enter into force.¹⁹ Even if this Protocol will not be a real game-changer, it does make some (small) steps forward in facilitating the gathering of digital evidence in a cross-border context. Furthermore, in December 2022, the Organisation for Economic Co-operation and Development (OECD) adopted a set of principles for government access to personal data held by private actors.²⁰ In addition, the United Nations (UN) has been working on this issue since 2019, with China, Russia and other states pushing for a UN convention.²¹ While there is no publicly available draft yet at the time of writing this introduction, many

¹⁴ Council of the EU, *Conclusions on Improving Criminal Justice in Cyberspace*, ST 10007/16 INIT (Brussels: Council of the EU, 9 June 2016).

¹⁵ Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services and amending Directive 2000/31/EC of 19 October 2022 (Digital Services Act) [2022] OJ L 277/1. For an analysis of the new obligations service providers have under the Digital Services Act, see, e.g., M. Walrave, C. Van de Heyning, V. Franssen, C. Mathys, J. Vrielink, M. Giacometti, A. Gilen and O. Gangi, *Cyberviolence: Defining Borders on Permissibility and Accountability – @ntidote 2.0*, Final Report (Brussels: Belgian Science Policy Office (BELSPO), 2023), 78–82, www.belspo.be/belspo/brain2-be/projects/FinalReports/Antidote_FinRep_en.pdf.

¹⁶ Council of Europe, Cybercrime Convention, ETS No. 185, 23 November 2001.

¹⁷ This introduction was finalised in early January 2024.

¹⁸ Council of Europe, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, ETS No. 224, Strasbourg, 12 April 2022 (Second Additional Protocol).

¹⁹ At the time of finalising this introduction, the Second Additional Protocol had been signed by forty-one states and ratified by two states (Serbia and Japan). It will enter into force when at least five states have ratified it.

²⁰ Organisation for Economic Co-operation and Development (OECD), *Declaration on Government Access to Personal Data Held by Private Sector Entities*, 2023, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>.

²¹ UN General Assembly, Resolution A/RES/74/247 on Countering the Use of Information and Communications Technologies for Criminal Purposes, 27 December 2019. For a recent analysis of the ongoing process and stakes, see, e.g., I. Wilkinson, 'What Is the UN Cybercrime Treaty and Why Does It Matter?', Chatham House, 2 August 2023, www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter.

stakeholders have already expressed deep concerns about the prospect of that UN Cybercrime Treaty.²²

At EU level, too, the legal situation regarding the collection of digital evidence has evolved considerably. By now, the European Investigation Order (EIO)²³ has become a commonly used instrument for gathering evidence in another member state, even though it still has the flaws that were identified years ago with respect to digital evidence.²⁴ More importantly, in July 2023 the so-called e-Evidence Regulation was promulgated after a long and difficult legislative process that was kicked off in April 2018.²⁵ This Regulation will bring about tangible changes by creating, for the first time, a direct cooperation mechanism between the judicial authorities of one member state and the service providers established or represented in another member state.²⁶

Nevertheless, a crucial part of the puzzle is still missing, namely, an agreement between the EU and the United States in the framework of the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which will lift the so-called blocking statute that prevents US-based service providers from sharing content data with judicial authorities in the EU and, conversely, national and EU blocking statutes for EU-based service providers.²⁷ The negotiations on the future US–EU CLOUD Act Agreement were kicked off in 2019, then stalled for quite a while as the EU first had to focus on an intra-EU compromise on the e-Evidence package. The negotiations restarted in March 2023 after that intra-EU compromise had been reached, though they promise to be challenging due to the systemic differences both between the US and the EU legal frameworks and among the EU member states.

Finally, at national level, the collection of digital evidence is regulated very differently from one legal system to another, as the national chapters in this volume adequately demonstrate. Whereas some legal systems have adjusted their legislation in a comprehensive way to enable

²² See, e.g., European Data Protection Supervisor, *Opinion 9/2022 on the Recommendation for a Council Decision Authorising the Negotiations for a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, adopted on 18 May 2022, https://edps.europa.eu/data-protection/our-work/publications/opinions/opinion-recommendation-council-decision-authorising_en; D. Brown, 'No Consensus on Proposed Global Cybercrime Treaty. A Flawed Treaty Could Empower Rights Abuses on a Global Scale', Human Rights Watch, 6 September 2023, www.hrw.org/news/2023/09/06/no-consensus-proposed-global-cybercrime-treaty. For several contributions assessing the different steps in the negotiations, see, e.g., Electronic Frontier Foundation (EFF), 'United Nations Cybercrime Treaty', www.eff.org/issues/un-cybercrime-treaty.

²³ Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L130/1.

²⁴ Tosza, 'Gathering Cross-Border Digital Evidence', 277; S. Tosza, 'All Evidence Is Equal, but Electronic Evidence Is More Equal Than Any Other: The Relation between the European Investigation Order and the European Production Order' (2020) 11(2) *New Journal of European Criminal Law* 161, 163–164; M. Giacometti, 'Collecte transfrontalière de preuves numériques selon le point de vue belge: La décision d'enquête européenne, un moyen approprié?', in V. Franssen and D. Flore (eds.), *Société numérique et droit pénal: Belgique, France, Europe* (Brussels: Bruylant, 2019), 296–297.

²⁵ European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, COM/2018/225 final – 2018/0108 (COD), 17 April 2018. For an analysis of the initial proposal, see V. Franssen, 'The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement', *European Law Blog*, 12 October 2018, <https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/>.

²⁶ For a more in-depth analysis of the new e-Evidence Regulation, see V. Franssen, 'Cross-Border Gathering of Electronic Evidence in the EU: Toward More Direct Cooperation under the e-Evidence Regulation', in V. Mitsilegas, M. Bergström and T. Quintel (eds.), *Research Handbook on EU Criminal Law*, 2nd ed. (Edward Elgar, 2024), 183–210; S. Tosza, 'Mutual Recognition by Private Actors in Criminal Justice? E-evidence Regulation and Service Providers as the New Guardians of Fundamental Rights' (2024) 61(1) *Common Market Law Review* 139–166; S. Tosza, 'The E-evidence Package Is Adopted: End of a Saga or Beginning of a New One?' (2023) 2 *European Data Protection Law Review* 168. See also Chapter 7 in this volume.

²⁷ For further analysis, see Franssen, 'Cross-Border Gathering of Electronic Evidence in the EU' at 205–207. See also Chapter 21 in this volume.

LEAs to face the reality of conducting criminal investigations in the digital era, others have amended their law only in a piecemeal way. Yet others are still discovering this new reality and grappling with terms and measures in this respect. With respect to the role of service providers in criminal investigations, the national chapters reveal highly disparate approaches too. Some states adhere strictly to a territorial approach, which prohibits them from cooperating with foreign service providers in a direct way, that is, without the intervention of the state where the service provider is established. Without surprise, this leads to a lot of frustration among LEAs, which feel insufficiently equipped to face present-day challenges in criminal investigations. In response to this frustration, certain legislators have chosen to impose data localisation and/or extensive data retention obligations upon service providers.²⁸ In other legal systems, the courts or legislators have extrapolated the approach laid down in Article 18(1)(b) of the Cybercrime Convention – which gives states the possibility to adopt legislation providing for a production order relating to subscriber information held by foreign service providers that offer services in their territory – to the production of other types of data. Some legal systems also simply reject the location of storage of the data as a determining criterion.²⁹

In addition to new legislation on criminal procedure and cross-border investigative measures, the gathering of digital evidence is also confronted, more than ever, with limits imposed by the data protection rules, both at national level and in a cross-border context. Whereas, for a long time, criminal procedure seemed to be shielded from data protection concerns – as state actors were convinced that the goals of criminal law necessarily prevail over the fundamental right to data protection – this has completely changed with the adoption of the General Data Protection Regulation (GDPR)³⁰ and the Law Enforcement Directive (LED).³¹ Despite both legal instruments having been applicable for several years now, the profound impact of the principles and rules they contain is only starting to become apparent. Notwithstanding the already huge body of case law of the Court of Justice of the European Union (CJEU) in this area, many questions remain unclear, such as the precise scope of application and interaction between the LED and the GDPR, and their interplay with new legal instruments such as the e-Evidence Regulation.

The influence of data protection law on the collection of digital evidence by LEAs is, however, crystal-clear when it comes to data retention obligations. The objective of such obligations is to make sure that personal data processed by private actors can still be produced to LEAs should the access to the data be deemed necessary in the course of a criminal investigation. Typically, such obligations are general and untargeted, meaning that no distinction is made between (potential) suspects and non-suspects. Indeed, LEAs argue that it is impossible to target certain (groups) of persons at the start of the data retention and insist that data retention is only a precautionary measure, which precedes a concrete criminal investigation. Notwithstanding this argument, the CJEU has ruled on several occasions that general data retention obligations regarding traffic data are incompatible with the Charter.³² In search of new solutions, some member states have adopted new legislation, attempting to meet the requirements of the CJEU. In other member

²⁸ See, e.g., Chapters 17 (China), 18 (Russia) and 19 (Turkey) in this volume.

²⁹ See, e.g., Chapter 9 (Belgium) in this volume. For further analysis, see also the comparative Chapter 16 in this volume.

³⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

³¹ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

³² See, e.g., Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and others* [2014] ECLI:EU:C:2014:238, para. 61; Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB* [2016] ECLI:EU:C:2016:970; Joined Cases C-511/18, C-512/18

states, surprisingly, the legislation has hardly changed throughout the years. This, too, leads to a fragmented legal landscape and substantial legal uncertainty, for both LEAs and service providers covered by data retention obligations, and it compromises the protection of citizens' fundamental rights.

THE HANDBOOK'S OBJECTIVES AND STRUCTURE

Considering the importance of digital evidence in criminal investigations and the numerous challenges its collection raises, the need for thorough legal analysis in this area cannot be underestimated. This handbook aims to address this need by offering an all-encompassing and intra-disciplinary analysis based on comparative research. In doing so, the book seeks to contribute to a better understanding of the problems and the solutions that have been so far adopted at different levels. It is the fruit of two interconnected research projects funded by the University of Liège, the European Commission and the Fund for Scientific Research of the French Community in Belgium (FRS-FNRS),³³ and the output of years of research conducted both before and after that research funding. What started as a small idea grew into a comprehensive multi-annual research agenda. This research would not have been possible without the cooperation of many excellent academic experts, coming from all over the world. Several of them contributed actively to this book; others were involved at some point of the research. Moreover, this research was supported and enriched by a fruitful dialogue with several stakeholders (involving LEAs, both Belgian and EU policymakers and industry representatives), who participated in one or more scientific events organised in the framework of the aforementioned research projects.³⁴

Both research projects, in essence, focused on the same problem regarding the collection of digital evidence: when LEAs seek to gather digital evidence, they are confronted with various challenges, due to quickly evolving technologies and the borderless nature of the internet, but also because the data they are looking for is often processed by private companies which are not necessarily located in the territory where the criminal investigation is being conducted.

and C-520/18, *La Quadrature du Net a.o.*, 6 October 2020, ECLI:EU:C:2020:791. For an overview of the Court's case law, see, e.g., B. Flumian and V. Franssen, 'Le nouveau cadre légal en matière de conservation des données électroniques: "Old wine in new bottles" pour les autorités judiciaires?', in V. Franssen and A. Masset (eds.), *Le droit pénal et la procédure pénale en constante évolution* (Liège: Anthemis, 2022), 321–329.

³³ The first project, entitled 'The Cooperation of ICT Companies in Criminal Investigations', was funded by the FRS-FNRS (research grant CDR J.0293.17) and the University of Liège with Vanessa Franssen as the principal investigator. The second research project, entitled 'Cross-Border Gathering of Digital Evidence: Mutual Legal Assistance, Its Shortcomings and Remedies', was co-funded by the European Commission (Marie Curie, FP7 people funding) and the University of Liège (postdoctoral grant BePD-COFUND) with Stanisław Tosza as the principal investigator.

³⁴ These events included: (1) a closed experts and stakeholders meeting ('Gathering of Digital Evidence: National and Transnational Challenges for Law Enforcement and Private Industry') organised on 28–29 June 2017; (2) a bilingual experts workshop on 'Cyberinvestigation and E-evidence: Legal and Technological Challenges', which took place on 12 March 2018, with the additional support of the David-Constant Foundation; (3) a research meeting on 5–6 April 2018 with academic experts ('The Cooperation of ICT Companies in Criminal Investigations: A Comparative Perspective'); and (4) an international conference on 25 and 26 November 2019, dedicated to 'Digital Evidence and Cooperation of Service Providers: Toward European and Global Solutions'. Additionally were organised, thanks to punctual funding of the ULiège, the URCité and the University of Luxembourg: (5) a panel on 'The End of Data Retention: Long Live the Protection of Fundamental Rights?' at the 14th International Conference on Computers, Privacy & Data Protection (CPDP) *Enforcing Rights in a Changing World* (Brussels, 27–29 January 2021); (6) an international research seminar entitled 'Criminal Justice and Digitalisation' (Liège, 16 May 2022); (7) a panel on 'The New E-evidence Regulation: Problem Solved or Opening of a Pandora's Box?' at the 16th International Conference on CPDP *Ideas That Drive Our Digital World* (Brussels, 24–26 May 2023); and (8) a panel on 'Digital Investigations and the Role of the Private Sector' at the conference 'Private Actors as Judges and Enforcers in the Technology-Driven World' (Luxembourg, 4–5 July 2023).

National, European and international legislation is often not sufficiently adjusted to account for these challenges, thus creating considerable uncertainty for LEAs and private actors, and ultimately also for the citizens whose data is compromised.

That said, each research project took a different perspective: the first project was bottom-up, centring on national legislation and practice and aimed at drawing workable solutions from comparative analysis, whereas the second one was conceived top-down, looking at the possibility of creating European-wide and transatlantic solutions. Both projects have therefore been complementary, contributing to the richness of the present book. All contributions in this book provide a unique take on one or more aspects relating to the gathering of digital evidence, whether from a national, a supranational or an international perspective, and have gone through a substantial editorial review process.

The book contains three main parts. Part I deals with specific topics relating to the gathering of digital evidence that merit a **transversal** and more in-depth approach.

In Chapter 1, **Anže Erbežnik** takes stock of a wide range of initiatives and policy programmes related to digitalisation and cybersecurity adopted by the EU in recent years, analysing the underlying philosophy. He also assesses the broader impact the increased attention for digital evidence has on the criminal justice system, in particular through the lens of privacy, judicial oversight and extraterritorial application of the law.

In Chapter 2, **Dan Svantesson** and **Anna-Maria Osula** decrypt the normative questions regarding jurisdiction that are triggered by the digital reality and the need for LEAs to have adequate access to digital evidence. Furthermore, they examine a range of piecemeal solutions that have been adopted to address these jurisdictional challenges.

Chapter 3 sees **Gavin Robinson** dig into the complex interaction between data protection law and criminal procedure. He unravels the current European legal framework and its implications for digital evidence gathering based on direct cooperation between public authorities and private actors.

In Chapter 4, **Cyprien Delpech de Saint Guilhem** explains the functioning of encryption technologies from a more technical point of view. He analyses the systemic risks of creating ‘back doors’ or otherwise weakening encryption, and explores possible pathways for legal access by LEAs in the future.

Next, in Chapter 5, **Giulia Lasagni** analyses the inherent characteristics of digital evidence that are relevant for the law of evidence. She also gives an overview of existing digital forensics standards and guidelines at international and European levels, and scrutinises the current European legal landscape on admissibility of evidence.

Tatiana Tropina takes the reader to the intersection between criminal procedure and national security in Chapter 6. She makes a comparison between data collection by LEAs, which is in principle targeted to a suspect, and bulk data collection by national security or intelligence agencies to analyse threats to and prevent attacks on national security.

In Chapter 7, **Theodore Christakis** analyses the new e-Evidence Regulation and Directive adopted by the EU in light of the diametrically opposite positions that were taken by the three EU institutions in the negotiation process. He shows how they eventually managed to untie the Gordian knot in this crucial piece of legislation to facilitate the cross-border preservation and production of data for evidence purposes.

And finally, in Chapter 8, **Angela Aguinardo** and **Paul de Hert** investigate how cross-border digital evidence gathering is regulated at the level of the Council of Europe. Whereas the options under the Cybercrime Convention were rather limited, the Second Additional Protocol’s purpose is to innovate by explicitly enabling cross-border direct cooperation between

LEAs and service providers for the collection of certain types of data. The proof of the pudding will, however, be in the eating: will this Protocol live up to the expectations?

In Part II, the Handbook takes a closer look at digital evidence gathering and the cooperation between LEAs and service providers in seven EU member states – **Belgium** (Chapter 9 by **Sem Careel** and **Frank Verbruggen**), **Estonia** (Chapter 10 by **Agnes Kasper**, **Eneli Laurits** and **Melita Sogomonjan**), **Germany** (Chapter 11 by **Dominik Brodowski**), **Ireland** (Chapter 12 by **T. J. McIntyre** and **Maria Helen Murphy**), **Luxembourg** (Chapter 13 by **Katalin Ligeti** and **Gavin Robinson**), **Poland** (Chapter 14 by **Maciej Rogalski**) and **Spain** (Chapter 15 by **Carmen Cuadrado Salinas** and **Juan Carlos Ortiz-Pradillo**). These legal systems were selected on the basis of several criteria: geographic diversity, diversity in legal families and strategic systems for service providers (Ireland), from the point of view of digitalisation (Estonia and Luxembourg) and in terms of being frontrunners in direct cooperation (Belgium).³⁵ These chapters are based on a detailed questionnaire and several rounds of discussion with the experts who wrote them. Their main purpose is to provide a coherent and comprehensive understanding of the state of play in the respective legal systems. These chapters study the deficiencies and the obstacles related to the gathering of digital evidence, and the solutions to these problems that are developed at the national level, as well as examining the influence of European law. Moreover, these chapters reflect on the future impact the new EU e-Evidence Regulation is likely to have on the respective national legal systems. The analysis integrates both ‘law in books’ and ‘law in action’, which is particularly precious for a subject matter that is often not regulated in an extensive way by legislation. The approach is multi-focal and intra-disciplinary, which means, on the one hand, that the chapters encompass the perspectives of LEAs, (national and foreign) service providers and citizens (including as regards the protection of their fundamental rights) and, on the other hand, that they take into consideration not just the law of criminal procedure but also the interplay with information technology (IT) law, data protection law and human rights law. Part II wraps up with a comparative analysis of the seven legal systems, in Chapter 16 by **Stanisław Tosza** and **Vanessa Franssen**, drawing inter-systemic conclusions on the collection of digital evidence in the EU.

The earlier-mentioned challenges relating to the gathering of digital evidence are, of course, not confined to the EU level. Across the globe, LEAs and service providers are confronted with quite similar problems. That is why, in the Part III of the handbook, we turn to five major, non-EU legal systems: **China** (Chapter 17 by **Li Zhe** and **Jin Zhenan**), **Russia** (Chapter 18 by **Maria Filatova**, **Olga Kostyleva** and **Tatiana Alekseeva**), **Turkey** (Chapter 19 by **Seçil Bilgiç**), the **United Kingdom** (Chapter 20 by **Elif Mendos Kuşkonmaz** and **Ian Walden**) and the **United States** (Chapter 21 by **Marine Corhay** and **Vanessa Franssen**). Each of these jurisdictions is particularly relevant, though for quite different reasons, for the cross-border gathering of digital evidence, both today and in the years to come. These chapters offer a unique insight into legal systems that are at the heart of the global debate.

In the handbook’s Conclusion, by **Vanessa Franssen** and **Stanisław Tosza**, is an assessment of current legal solutions that are offered at the national, European and international levels to the challenges encountered in the area of digital evidence. The Conclusion evaluates whether these solutions create more legal certainty for all involved stakeholders (LEAs, service providers and citizens), while striking a balance between effective law enforcement and fundamental rights protection. Furthermore, it looks to the future, by highlighting new challenges and suggesting further pathways for elaborating constructive solutions to unanswered dilemmas in this field.

³⁵ Initially, the pool of countries also included Finland and France, but the national experts were unfortunately unable to provide a full analysis for this book.

FUTURE PERSPECTIVES

Since the initial ideas (going back to a paper written in 2015)³⁶ and the conception of the above-mentioned research projects, the world has changed a lot. So have the national, EU and international legal frameworks on the matter of gathering digital evidence, especially in cross-border situations. Still, the challenges and the needs remain largely the same, even if technologies continue to evolve.³⁷

In sum, the book appears as the EU and the Council of Europe have just adopted new legislation that seeks to effectively overcome certain obstacles to gathering certain types of digital evidence in a cross-border context. The impact of this new legislation will only become clear in several years, and only after the necessary national legislative work completes the jigsaw puzzle. Moreover, the new European legislation is largely limited to the preservation and production of data; it does not address other issues such as encryption and the advent of evermore sophisticated AI tools. Neither does it regulate a whole range of other investigative measures that are already used by LEAs at national level, or other kinds of cooperation duties of service providers (such as the duty to provide technical assistance or to remove illegal content). National diversity remains high in that respect. Therefore, the global debate on the role of service providers in the context of criminal investigations and the challenges raised by the gathering of digital evidence will remain vivid for many years to come.

³⁶ V. Franssen and K. Ligeti, *The Cooperation of Internet and Other Service Providers with Judicial Authorities: National Report on Luxembourg*, 2015, 4, https://orbi.uliege.be/bitstream/2268/201353/1/Report_Luxembourg_Franssen%26Ligeti_Publication.pdf.

³⁷ For instance, in 2015 the challenges created by artificial intelligence (AI) were not yet considered pressing, whereas today AI tools are deployed in nearly all areas of society and likely to revolutionise the law of criminal procedure too. See, e.g., V. Franssen and A. Berrendorf, 'The Use of AI Tools in Criminal Courts: Justice Done and Seen to Be Done?' (2021) 92 *Revue internationale de droit pénal* 199.

PART I

Collecting Digital Evidence

Transversal Challenges and Solutions

Impact of Digital Evidence Gathering on the Criminal Justice System

A Broader Perspective

Anže Erbežnik

1.1 INTRODUCTION

The digital age is presenting humankind with unprecedented opportunities as well as challenges. On the one side, digitalisation offers benefits in terms of learning, interconnectivity, cost reduction, online work, help from artificial intelligence (AI) and so on, metaphorically changing ‘homo sapiens’ into ‘homo deus’.¹ However, on the other side, it gives the possibility of permanent and unlimited control over and manipulation of individuals (voting behaviour, public opinion, consumer habits), not only by governments but also by private entities. We are leaving our digital fingerprints on a daily basis. The one that controls such mass data controls society and can use it to influence the future.² This is especially true because AI allows for the analysis and profiling of enormous amounts of data. Two different patterns emerge in the world, one based on permanent control and technological dictatorship,³ the other based on technological democracy.⁴ Digitalisation of criminal justice forms only a part of digitalisation generally, although an important one. The area of criminal justice is, metaphorically speaking, the second (hidden) face of the Greek god Janus. In the criminal justice area, governments proverbially replace ‘the carrot with the stick’. Therefore, criminal justice shows early warning of possible negative trends in society. The imbalance between technological possibilities and the legal limits applied to them could

¹ See Y. N. Harari, *Homo Deus: A Brief History of Tomorrow* (New York: Harper, 2017).

² Prediction models are based on the Bayes theorem (the probability of an event based on prior knowledge of conditions that might be related to the event) and game theory. For basic understanding, see M. Gr. Voskoglou, ‘Bayesian Reasoning and Artificial Intelligence’ (2020) 17 *WSEAS Transactions on Advances in Engineering Education* 92–98; W. Von der Linden, V. Dose and U. von Toussaint, *Bayesian Probability Theory* (Cambridge: Cambridge University Press, 2014); J. Von Neumann and O. Morgenstern, *Theory of Games and Economic Behaviour*, 3rd ed. (Princeton, NJ: Princeton University Press, 1953); B. Bueno de Mesquita, ‘Thinking Inside the Box: A Closer Look at Democracy and Human Rights’ (2005) 49(3) *International Studies Quarterly* 439–457; B. Bueno de Mesquita, *The Predictioneer’s Game* (New York: Random House, 2010). See also the Cambridge Analytica scandal on the misuse of Facebook data and an attempt to try to influence voters. On this scandal, see, e.g., Resolution 2018/2855(RSP) of the European Parliament of 25 October 2018 on the use of Facebook users’ data by Cambridge Analytica and the impact on data protection, [2018] OJ C 345, 16 October 2020.

³ It is the creation of a system whereby Orwell’s Big Brother meets Huxley’s Brave New World. See, e.g., A. Kendall-Taylor, E. Frantz and J. Wright, ‘The Digital Dictators: How Technology Strengthens Autocracy’, *Foreign Affairs*, 6 February 2020, www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators; D. Carpi, *Law and Culture in the Age of Technology* (Berlin: De Gruyter, 2022) 59–76; K. Manheim and L. Kaplan, ‘Artificial Intelligence: Risks to Privacy and Democracy’ (2019) 21 *Yale Journal of Law & Technology* 106–186; H. A. Ünver, ‘Artificial Intelligence, Authoritarianism and the Future of Political Systems’, *EDAM*, 30 July 2018, <https://edam.org.tr/en/4025-2/>; E. Snowden, *Permanent Record* (New York: Metropolitan Books, 2020).

⁴ See also four possible model future scenarios for a digital Europe: EUtopia, EUsed, EUSSR and EUniformity. Monitor Deloitte, *Digital Transformation in the EU 2035: A Glimpse into the Future* (July 2019), www2.deloitte.com/content/dam/Deloitte/de/Documents/strategy/deloitte-future-of-digital-transformation-eu-2035.pdf.

create a fully fledged preventive state (in the negative sense), posing a threat to civil liberties and democracy. Prevention has been part of police work since the nineteenth century when the first police forces emerged.⁵ However, modern technology coupled with AI provides the possibility and the temptation to go much further and to detect ‘suspicious’ or ‘anti-social’ behaviour early on, basically at the stage of the Orwellian notion of ‘thoughtcrime’.⁶

The intention of this chapter is to present the existing European Union (EU) philosophy when it comes to digitalisation, specifically in relation to cross-border cooperation in criminal justice. Based on such philosophy, a new set of concepts has been developed and applied to concrete legislative instruments. It is not about a single instrument but about the same logic being applied to a whole variety of them. It clearly shows a trend challenging the classical notion of the right to privacy and raises the question of whether a new concept of privacy is necessary in the digital age. In terms of the legal questions raised, two are of specific interest to cross-border cooperation in EU criminal law in the digital age, namely the issues of judicial (court) oversight and extraterritorial application of law. Therefore, firstly, a general overview of the latest EU digital and security strategies is provided (Sections 1.2.1 and 1.2.2), together with a short analysis of specific legislative instruments connected with them and relevant for the criminal justice area (Section 1.2.3). Secondly, a historical analysis of the right to privacy as the main affected right by digitalisation follows, together with its modern understanding. Privacy concepts initially developed by case law of the US Supreme Court and adapted by case law of the European Court of Human Rights (ECtHR) are presented (Section 1.3). Lastly, specific aspects of digitalisation in the area of EU justice are addressed (Section 1.4) before a brief conclusion is offered (Section 1.5).

1.2 DIGITALISATION IN THE AREA OF EU CRIMINAL JUSTICE

1.2.1 *The EU Digital Strategy*

An evaluation of interconnected policies and instruments is necessary to get a picture of EU digitalisation from a criminal justice perspective. In 2010, the EU adopted its first comprehensive ten-year ‘Digital Agenda for Europe’⁷ as part of the ‘Europe 2020 Strategy’,⁸ one of its seven

⁵ See A. Ashworth and L. Zedner, ‘The Historical Origins of the Preventive State’, in *Preventive Justice* (Oxford: Oxford University Press: 2014), 27–50; A. Ashworth and L. Zedner, ‘The Rise and Restraint of the Preventive State’ (2019) 2 *Annual Review of Criminology* 429–450; C. Steiker, ‘The Limits of the Preventive State’ (1998) 88(3) *Journal on Criminal Law and Criminology* 771–808.

⁶ For example, the passenger name record (PNR) system of collecting and analysing the data of air travellers (Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, [2016] OJ L 119, 4 May 2016); anti-money laundering rules (Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, [2015] OJ L 141, 5 June 2016; and replaced in the future by a new regulation and directive); criminalisation of travelling for purposes of terrorism (Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, [2017] OJ L 88, 31 March 2017); and so on. These are all instruments with elements of the preventive state.

⁷ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on A Digital Agenda for Europe, [2010] (COM(2010) 245 final), 19 May 2010 (A Digital Agenda for Europe). See also Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on The Digital Agenda for Europe – Driving European Growth Digitally, [2012] (COM(2012) 784 final), 18 December 2012.

⁸ European Commission, Communication on Europe 2020: A Strategy for Smart, Sustainable and Inclusive Growth, [2010] (COM(2010) 2020 final), 3 March 2010.

flagship initiatives.⁹ It highlighted the link between digitalisation, security and justice, stating that “[p]eople’s enjoyment of digital technologies, be it as citizens, consumers or workers, is marred by privacy and security concerns”.¹⁰ It pointed to rising cybercrime and the risk of low trust in networks as the main obstacles, and introduced ‘Trust and Security’ as one of the action areas.¹¹ However, security was only one aspect among many others. The 2010 Digital Agenda was followed in 2020 by ‘Shaping Europe’s Digital Future’,¹² a five-year programme that is more security-oriented. It refers, inter alia, to ‘building synergies between civilian cyber resilience and the law enforcement and defence dimensions of infrastructures’.¹³ This shows a trend for partnerships between private companies and law enforcement as will be elaborated later in this chapter. Under four headings,¹⁴ the 2020 Digital Agenda envisages actions and legislative work on AI, broadband internet, cybersecurity and a single market, digital education, taxation, industry, data strategy, digital identity, media, electronic health records and so on. In addition, it provides for a whole set of (sub)strategies and agendas, for example a white paper on AI,¹⁵ an updated Action Plan on 5G and 6G,¹⁶ an EU governments interoperability strategy,¹⁷ a European Data Strategy,¹⁸ a Consumer Agenda,¹⁹ a Media and Audiovisual Action Plan,²⁰ a European Democracy Action Plan,²¹ a Cybersecurity Strategy,²² a European Pillar of Social

⁹ The other six being ‘Innovation Union’, ‘Youth on the Move’, ‘Resource Efficient Europe’, ‘An Industrial Policy for the Globalisation Era’, ‘An Agenda for New Skills and Jobs’ and ‘European Platform against Poverty’.

¹⁰ A Digital Agenda for Europe, p. 5.

¹¹ It was stated that the digital age shall be neither ‘Big Brother’ nor ‘Cyber Wild West’. The following actions were envisaged: modernising the European Network and Information Security Agency (ENISA) and devising measures to allow faster reactions to cyberattacks; launching legislative initiatives to combat cyberattacks and rules on jurisdiction in cyberspace; working with global stakeholders; exploring the extension of security breach notification provisions; producing guidance for the implementation of a new Telecoms Framework with regard to the protection of individuals’ privacy and personal data; supporting reporting points for illegal content online and awareness campaigns on online safety for children; and fostering multi-stakeholder dialogue and self-regulation of service providers.

¹² Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Shaping Europe’s Digital Future, [2020] (COM(2020) 67 final), 19 February 2020.

¹³ Ibid., p. 5.

¹⁴ Namely, ‘Technology That Works for People’, ‘A Fair and Competitive Economy’, ‘An Open, Democratic and Sustainable Society’ and ‘International Dimension’.

¹⁵ European Commission, White Paper on Artificial Intelligence – A European Approach to Excellence and Trust, [2020] (COM(2020) 65 final), 19 February 2020.

¹⁶ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 5G for Europe: An Action Plan, [2016] (COM(2016) 588 final), 14 September 2016 (with subsequent changes).

¹⁷ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on European Interoperability Framework – Implementation Strategy, [2017] (COM/2017/0134 final), 23 March 2017 (with subsequent changes).

¹⁸ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on A European Strategy for Data, [2020] (COM(2020) 66 final), 19 February 2020.

¹⁹ Communication from the Commission to the European Parliament and the Council on the New Consumer Agenda Strengthening Consumer Resilience for Sustainable Recovery, [2020] (COM/2020/696 final), 13 November 2020.

²⁰ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Europe’s Media in the Digital Decade: An Action Plan to Support Recovery and Transformation, [2020] (COM(2020) 784 final), 3 December 2020.

²¹ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Democracy Action Plan, [2020] (COM/2020/790 final), 3 December 2020.

²² Joint Communication to the European Parliament and the Council on the EU’s Cybersecurity Strategy for the Digital Decade, [2020] (JOIN(2020) 18 final), 16 December 2020.

Rights Action Plan²³ and so on. In 2021 the Digital Agenda was complemented with a ten-year ‘Digital Compass’.²⁴ The Compass provides for clear targets in terms of: (1) a digitally skilled population and highly skilled digital professionals; (2) secure and performant sustainable digital infrastructures; (3) digital transformation of businesses; and (4) digitalisation of public services. In addition, in 2022 the Commission proposed a ‘European Declaration on Digital Rights’.²⁵ Such a development was pre-empted by a non-binding Lisbon Declaration on Digital Rights proposed by the EU Council Portuguese presidency,²⁶ and by a Decision establishing the 2030 Policy Programme ‘Path to the Digital Decade’.²⁷ The latter Decision also sets out a monitoring and cooperation mechanism for the programme, which includes an obligation for the three main institutions and the member states to cooperate on general objectives at the Union level.²⁸

The main EU focus is on the benefits of a digital society. For example, the European Data Strategy states that ‘[d]ata will reshape the way we produce, consume and live. Benefits will be felt in every single aspect of our lives, ranging from more conscious energy consumption and product, material and food traceability, to healthier lives and better health-care.’²⁹ The intention is to create a European way of data governance by ‘balancing the flow and wide use of data, while preserving high privacy, security, safety and ethical standards’.³⁰ The European Data Strategy specifically refers to electronic evidence (e-evidence) and extraterritorial application of laws. However, there is a certain contradiction as, on one side, the intention is to get the highest added value from (mass) data, including its use for AI, while, on the other side, utmost respect for privacy, data protection and fundamental rights is proclaimed.

Several legislative instruments relate to the Digital Strategy,³¹ for example the Digital Markets Act,³² the Digital Services Act (DSA),³³ the EU Data Act,³⁴ the Data Governance Act,³⁵ the AI

²³ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Pillar of Social Rights Action Plan, [2021] (COM(2021) 102 final), 4 March 2021.

²⁴ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the 2030 Digital Compass: The European Way for the Digital Decade, [2021] (COM(2021) 118 final), 9 March 2021.

²⁵ European Commission, European Declaration on Digital Rights and Principles, [2022] (COM(2022) 28 final), 26 January 2022.

²⁶ Portuguese Presidency of the Council of the European Union, ‘Lisbon Declaration – Digital Democracy with a Purpose’, 1 June 2021, www.lisbondeclaration.eu.

²⁷ Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, [2022] OJ L 323, 19 December 2022, p. 4.

²⁸ Article 2 of Decision (EU) 2022/2481. From a justice perspective, the following is important: to promote a human-centered and fundamental rights-based, inclusive, transparent and open digital environment; to ensure that online participation in democratic life is possible for everyone; to facilitate fair and non-discriminatory conditions for users; to improve resilience to cyberattack.

²⁹ European Data Strategy, 2.

³⁰ Ibid., 3.

³¹ See footnote 12.

³² Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), [2022] OJ L 265, 12 October 2022, p. 1.

³³ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act – DSA), [2022] OJ L 277, 27 October 2022, p. 1.

³⁴ Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), [2023] COM(2022) OJ L 2023/2854, 22 December 2023.

³⁵ Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), [2022] OJ L 152, 3 June 2022, p. 1.

Act³⁶ and the EU Media Freedom Act.³⁷ Some of these instruments have stirred up a certain amount of controversy, too. For example, the Digital Services Act introduces a harmonised framework for providers to deal with illegal content. It establishes the possibility of cross-border orders to act against illegal content and to provide information on it,³⁸ and introduces a presumption that foreign providers offering services in the Union are ‘domestic’ providers who have to nominate a legal representative.³⁹ In relation to cross-border removal of illegal content, it is based on a similar logic to e-evidence, discussed further in Section 1.3.1.⁴⁰ Some non-governmental organisations (NGOs) and legislators⁴¹ have raised criticisms in view of possible ‘censorship’. There is no common EU notion of illegal content.⁴² Only specific aspects of illegal content are addressed in EU legislation⁴³ and a debate to include hate speech under Article 83(1) is ongoing.⁴⁴ Further, questions exist on the foreseen crisis response management,⁴⁵ mitigating risk measures⁴⁶ and trusted flaggers.⁴⁷

³⁶ European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act – AI Act), [2021] (COM(2021) 206 final), 21 April 2021. The agreed text can be found under www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html. See, specifically, several exemptions to profiling and real-time remote biometric identification in Article 5 and Annex III. In that regard, the legislation left too many issues undefined and open, contradicting the principle of legal certainty.

³⁷ Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act), [2022] OJ L 2024/1083, 17 April 2024.

³⁸ DSA, Arts. 9 and 10. It is not clear how orders to act (Art. 9) will coexist with other EU instruments such as on terrorist content online. Member states could achieve the same goal (blocking or removal) by using the easier avenue of DSA administrative orders. The same applies to the coexistence of e-evidence in view of DSA information orders (Art. 10) for production of subscriber data.

³⁹ DSA, Art. 13.

⁴⁰ See, in particular, Chapter 7 in this volume.

⁴¹ Patrick Breyer, Rapporteur for Opinion, EP Committee on Civil Liberties, Justice and Home Affairs (LIBE), stated:

The new set of rules does not deserve the name “Digital Constitution”, because the deal fails in protecting our fundamental rights on the net. ... Freedom of expression is not protected from error-prone censorship machines (upload filters), arbitrary platform censorship and cross-border content removal orders from illiberal EU Member States without judicial approval, in effect making perfectly legally published media reports and information removable by referring to problematic national laws. (www.patrick-breyer.de/en/digital-service-act-shows-eus-unwillingness-to-take-digital-age-into-its-own-hands/)

⁴² Illegal content is defined in Art. 3(h) DSA as ‘any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law’.

⁴³ For example, child pornography in Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, [2011] OJ L 335, 17 December 2011; terrorist content online in Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, [2021] OJ L 172, 17 May 2021; and racism and xenophobia in Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, [2008] OJ L 328, 6 December 2008.

⁴⁴ Communication from the Commission to the European Parliament and the Council on A More Inclusive and Protective Europe: Extending the List of EU Crimes to Hate Speech and Hate Crime, [2021] (COM(2021) 777 final), 9 December 2021. See also N. Peršak, ‘Criminalising Hate Crime and Hate Speech at EU Level: Extending the List of Eurocrimes under Article 83(1) TFEU’ (2022) 33(2) *Criminal Law Forum* 85–119.

⁴⁵ DSA, Rec. 91 and Art. 36. It allows limiting freedom of expression by applying measures to ‘prevent, eliminate or limit any such contribution to the serious threat identified’.

⁴⁶ DSA, Art. 35.

⁴⁷ DSA, Art. 22. Such status will be given to an applicant that has demonstrated that it has particular expertise and competence for detecting, identifying and notifying illegal content, is independent from online platforms and carries out its activities diligently, accurately and objectively. Such flaggers will have priority in handling their requests. However, critics have warned about the potential for misuse. See Paul Meosky, ‘Europe’s Digital Services Package: What It Means for Online Services and Big Tech’, *EPIC*, 23 August 2022, <https://epic.org/europes-digital-services-package-what-it-means-for-online-services-and-big-tech/>.

The DSA is just one of the examples illustrating the important legal and political questions raised within digitalisation. However, the EU digital policies have to be understood together with the security part of digitalisation, namely the European Security Strategy.

1.2.2 *EU Security Union Strategy: A Question of Balance*

In 2020 a five-year ‘EU Security Union Strategy’⁴⁸ was proposed following the 2015 ‘European Agenda on Security’⁴⁹ and the 2010 ‘Internal Security Strategy’,⁵⁰ and coupled with several additional sub-strategies/action plans.⁵¹ To a large extent, it is focused on prevention (as its first objective suggests: ‘Building capabilities and capacities for early detection, prevention and rapid response to crises’⁵²), as well as on private–public partnerships (third objective: ‘Linking all players in the public and private sectors in a common effort’⁵³). In comparison with previous strategies, it seems more security prone, stating that ‘[s]ecurity is not only the basis for personal safety, it also protects fundamental rights and provides the foundation for confidence and dynamism in our economy, our society and our democracy’.⁵⁴ E-evidence is specifically mentioned under the title ‘Tackling evolving threats’. It states:

Electronic information and evidence is needed in about 85% of investigations into serious crimes, while 65% of the total requests go to providers based in another jurisdiction. The fact that traditional physical traces have moved online further expands the gap between the law enforcement and criminals’ capabilities. Putting in place clear rules for cross-border access to electronic evidence for criminal investigations is essential. This is why swift adoption by the European Parliament and Council of the e-evidence proposals is key

⁴⁸ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy, [2020] (COM(2020) 605 final), 24 July 2020. See also T. Wahl, ‘New EU Security Union Strategy’ (2020) 2 *Eu crim* 71–72; Resolution 2020/2791 (RSP) of the European Parliament of 17 December 2020 on the EU Security Union Strategy, [2020] OJ L 445, 29 October 2020; Europol, European Union Serious and Organised Crime Threat Assessment (SOCTA) Report, 2021; Council of the European Union, Council Conclusions on the Permanent Continuation of the EU Policy Cycle for Organised and Serious International Crime: EMPACT 2022+, 7100/23, 9 March 2023; Communication from the Commission to the European Parliament and the Council on the Fifth Progress Report on the Implementation of the EU Security Union Strategy, [2022] (COM(2022) 745 final), 13 December 2022.

⁴⁹ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Agenda on Security, [2015] (COM(2015) 185 final), 28 April 2015. See also supplementing communications on Implementing the European Agenda on Security: EU Action Plan Against Illicit Trafficking in and Use of Firearms and Explosives, [2015] (COM(2015) 624 final), 2 December 2015, and on Delivering on the European Agenda on Security to Fight against Terrorism and Pave the Way towards an Effective and Genuine Security Union, [2016] (COM(2016) 230 final), 20 April 2016.

⁵⁰ Council of the European Union, Draft on Internal Security Strategy of the European Union, Towards a European Security Model, 5842/2/2010, 23 February 2010.

⁵¹ For example, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on EU Strategy for a More Effective Fight against Child Sexual Abuse, [2020] (COM(2020) 607 final), 24 July 2020; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on EU Agenda and Action Plan on Drugs 2021–2025, [2020] (COM/2020/606 final), 24 July 2020; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Action Plan on Firearms Trafficking 2021–2025 (COM/2020/608 final); and Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to Tackle Organised Crime 2021–2025, [2021] (COM/2021/170 final), 14 April 2021.

⁵² EU Security Union Strategy, p. 5, <https://eur-lex.europa.eu/legal-content/EN/TEXT/PDF/?uri=CELEX:52020DC0605&from=EN>.

⁵³ Ibid.

⁵⁴ Ibid., p. 1.

to provide practitioners with an efficient tool. Cross-border access to e-evidence through multilateral and bilateral international negotiations is also key, to establish compatible rules at international level.⁵⁵

Further, the Commission counts on combining big data and AI in the security area, stating that '[a]rtificial intelligence could act as a powerful tool to fight crime, creating enormous investigative capabilities by analysing large amounts of information and identifying patterns and anomalies. It can also provide concrete tools, such as to help identify online terrorist content, discover suspicious transactions in the sales of dangerous products or offer assistance to citizens in emergencies.'⁵⁶ Fundamental rights are mentioned mainly under *ex post* human review. By reference to e-evidence, the benefits of data retention are proclaimed.⁵⁷ One of the main focal points is the fight against illegal content online with intended public–private cooperation and legislation on countering illegal hate speech online (DSA).

In comparison, the 2015 European Agenda on Security had more focus on fundamental rights by promoting democratic accountability and the better use of existing instruments.⁵⁸ This shift of focus by the new 2020 strategy and the legislative proposals connected with it raises certain concerns. The danger exists to create, as a 'third European way', a kind of unintended hybrid between a full-fledged preventive state and a 'lip-service' democracy (meaning democracy in name only). It can also further blur the lines between the private sector and the public authorities, whereby also blurring their duties and obligations.

1.2.3 Overview and Analysis of Specific Legislative Instruments at the Crossroads of Digitalisation and Criminal Justice

In parallel with the new security and digital strategies, or as a consequence of them, several legislative instruments affecting the online world were proposed or adopted. They build on similar concepts such as direct cross-border orders, private–public partnerships and transformation of private providers into 'state agents'. The following instruments will be briefly analysed: the newly adopted e-evidence package, the Regulation on terrorist content online (TCO) and the so-called e-privacy derogation for the purpose of combating sexual abuse of children online. Those instruments provide for efficiency but raise data protection and privacy issues and diminish the importance of the classical concept of judicial cooperation and its safeguards, especially on the territory of the executing/enforcing state.

⁵⁵ Ibid., p. 12.

⁵⁶ Ibid.

⁵⁷ It states:

Access to digital evidence also depends on the availability of information. If the data is erased too quickly, important evidence may disappear, so that the possibility to identify and locate suspects and criminal networks (as well as victims) no longer exists. On the other hand, data retention schemes raise questions of protection of privacy. Depending on the outcome of the cases pending before the European Court of Justice, the Commission will assess the way forward on data retention. (Ibid.)

However, the problem is that infringement proceedings were not started against member states that were not respecting Court of Justice of the European Union (CJEU) case law on data retention. For an overview of such case law, see Chapter 6 in this volume.

⁵⁸ The 2015 European Agenda on Security (p. 3) stated that '[a]ll security measures must comply with the principles of necessity, proportionality and legality, with appropriate safeguards to ensure accountability and judicial redress. The Commission will strictly test that any security measure fully complies with fundamental rights whilst effectively delivering its objectives.'

1.2.3.1 The ‘e-Evidence’ Legislative Package

Due to development of technology, the volatility of electronic data and the need for rapid cooperation, the Commission proposed two instruments forming the ‘e-evidence’ package,⁵⁹ namely a Regulation (e-Evidence Regulation)⁶⁰ and a Directive (e-Evidence Directive),⁶¹ and radically changing the understanding of mutual recognition in EU criminal law. The Regulation is based on Article 82 of the Treaty on the Functioning of the European Union (TFEU) (mutual recognition), and the Directive on Articles 53 and 62 TFEU (harmonisation of laws or other regulations in member states on the establishment and provision of services). The new system is based on certain ‘pan-European orders’ that are valid throughout the EU and is addressed directly to telecommunication service providers. It is also based on a presumption that foreign providers offering services in the Union are established in the EU.⁶² Therefore, they have to appoint a special representative in the EU. The new logic implies direct contact between judicial authorities from one member state and private service providers from another, generally without the participation of the executing/enforcing state’s authority. It also introduces extraterritorial application of law and thereby redefines the national territoriality and sovereignty of member states and third states. Consequently, interference with fundamental rights on the territory of other states is possible, without their knowledge and the possibility to object to it. This approach is not entirely new. Indeed, there is already a trend in some member states to understand national orders in connection with electronic evidence in a broader sense.⁶³ In parallel, there is also an ongoing procedure on the ratification of the Second Additional Protocol to the Budapest Cybercrime Convention,⁶⁴ and on negotiations for an agreement with the US regarding e-evidence.⁶⁵ A system of direct orders raises substantial issues in view of different standards on privacy and data protection, for example as regards data retention, court authorisations, types of electronic data, necessary levels of suspicion, types of offence for which data can be requested, rules regarding admissibility of evidence and so on.

⁵⁹ Considering that the EU legislative package on e-evidence will be analysed in more detail in Chapter 7 of this volume, this section provides only a short introduction to EU e-evidence, highlighting some specific issues.

⁶⁰ European Commission, Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (e-Evidence Regulation), [2018] (COM/2018/225 final), 17 April 2018. For the final agreed text, see Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (e-Evidence Regulation), [2023] OJ L 191, 28 July 2023, p. 118.

⁶¹ European Commission, Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (e-Evidence Directive), [2018] (COM/2018/226 final), 17 April 2018. For the final agreed text, see Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (e-Evidence Directive), [2023] OJ L 191, 28 July 2023, p. 181.

⁶² e-Evidence Regulation, Art. 3(4) and e-Evidence Directive, Art. 2(3).

⁶³ See Chapter 9 in this volume.

⁶⁴ Council Decision (EU) 2022/722 of 5 April 2022 authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, [2022] OJ L 134, 11 May 2022, p. 15. After the decision on signature, a second one followed on the ratification. The European Parliament gave its consent to the second decision on 17 January 2023. See European Parliament legislative resolution on the draft Council decision authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, [2023] (P9_TA(2023)0002), 17 January 2023.

⁶⁵ Council Decision of 6 June 2019 authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Council EU, doc. 9114/19.

The e-Evidence Regulation is envisaged for gathering all types of e-evidence in criminal proceedings.⁶⁶ Two types of order exist, namely a European Production Order⁶⁷ and a European Preservation Order.⁶⁸ They are intended for historical electronic data only, not for real-time interceptions, and complement⁶⁹ Directive 2014/41/EU on the European Investigation Order (EIO Directive).⁷⁰ The Commission proposed initially four categories of electronic data, namely: (1) subscriber data, (2) access data, (3) transactional data and (4) content data. Unlike the classical categories of such data, as known by national legislations and the Budapest Cybercrime Convention (subscriber data, traffic data and content data), a new category of ‘access data’ had been proposed, with an unclear delimitation from traffic/transactional data.⁷¹ However, in the final text the classical three categories were kept, while acknowledging a special treatment for data denominated as ‘data requested for the sole purpose of identifying the user’ (such as internet protocol (IP) addresses, source ports, time stamps and so on).⁷² The division is essential in view of the issuing authority since orders for subscriber data and data requested for the sole purpose of identifying the user as well as preservation orders can be issued or validated by prosecutors, whereas orders for traffic and content data can only be issued or validated by courts.⁷³ The division also affects the type of criminal offences for which an order can be issued. Orders for subscriber data and data requested for the sole purpose of identifying the user, as well as preservation orders, can be issued for all offences. Orders for traffic data and content data can be issued only for certain offences, namely for offences punishable above three years and certain enumerated offences.⁷⁴ The service provider must provide the data within ten days and in urgent circumstances within eight hours, or preserve it for sixty days with the possibility of an extension for thirty days.⁷⁵ The provider can decline the transfer only if the certificate is incomplete, contains manifest errors or

⁶⁶ According to Art. 3, point 8, e-evidence Regulation, ‘electronic evidence’ means ‘subscriber data, traffic data or content data stored by or on behalf of a service provider, in an electronic form, at the time of receipt of a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR)’.

⁶⁷ According to Art. 3, point 1, e-evidence Regulation, ‘European Production Order’ means

a decision ordering the production of electronic evidence, issued or validated by a judicial authority of a Member State in accordance with Article 4(1), (2), (4) and (5), and addressed to a designated establishment or to a legal representative of a service provider offering services in the Union, where that designated establishment or legal representative is located in another Member State bound by this Regulation.

⁶⁸ According to Art. 3, point 2 e-evidence Regulation, ‘European Preservation Order’ means

a decision which orders the preservation of electronic evidence for the purposes of a subsequent request for production, and which is issued or validated by a judicial authority of a Member State in accordance with Article 4(3), (4) and (5), and addressed to a designated establishment or to a legal representative of a service provider offering services in the Union, where that designated establishment or legal representative is located in another Member State bound by this Regulation.

⁶⁹ E-evidence Regulation, Art. 32.

⁷⁰ Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (EIO Directive), [2014] OJ L 30, 1 May 2014, p. 1.

⁷¹ Art. 2, point 8, of the initial Commission proposal (see footnote 60) defined ‘access data’ as

data related to the commencement and termination of a user access session to a service, which is strictly necessary for the sole purpose of identifying the user of the service, such as the date and time of use, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the user of a service, data identifying the interface used and the user ID. This includes electronic communications metadata.

The last sentence caused an unclear differentiation from traffic/transactional data.

⁷² E-evidence Regulation, Art. 2, points 8 to 12.

⁷³ *Ibid.*, Art. 4.

⁷⁴ *Ibid.*, Arts. 5 and 6. Such specific offences include offences from EU directives on combating fraud and counterfeiting of non-cash means of payments, abuse against children, cybercrime and terrorism.

⁷⁵ *Ibid.*, Art. 10(1)–(4) and Art. 11(1).

does not contain sufficient information, due to force majeure, or because from the sole information in the certificate it seems that the execution could interfere with immunities and privileges, or with rules on the determination or limitation of criminal liability relating to freedom of the press or freedom of expression under the law of the enforcing state.⁷⁶ Only in the case of non-compliance with the order can the issuing state turn to the enforcing state, which is supposed to compel the provider.⁷⁷ Moreover, a special procedure as regards conflicts of law with third countries is foreseen.⁷⁸ The EU Council followed suit in its general approach with some modifications to the original proposal.⁷⁹ It widened the scope to the execution of custodial sentences or detention orders of at least four months, following criminal proceedings, imposed by a decision that was not rendered in absentia, in cases where the person convicted absconded from justice.⁸⁰ It also introduced the possibility of a subsequent judicial approval in urgent circumstances and removed any assessment of fundamental rights by service providers. Those changes were confirmed in the final text. Furthermore, it introduced a consultation procedure for traffic/transactional data in cases which are not considered internal ('non-domestic cases'),⁸¹ and a very limited notification of the enforcing state regarding content data in cases not considered domestic but without suspensive effect.⁸²

On the other hand, the European Parliament proposed initially significant changes to the Commission proposal.⁸³ It included a substantive notification system with suspensive effect and the possibility of a reaction by the enforcing state, at least for more sensitive categories of data. It followed the EIO model, in particular on non-recognition grounds (including a fundamental rights non-recognition ground). In doing so, it deleted the new category of 'access data' proposed by the Commission, and distinguished between different data categories, depending on their invasiveness. It proposed direct transfers in the case of subscriber data, data for the sole purposes of identifying the user and preservation orders, and a notification procedure with suspensive effect for traffic and content data. However, if no answer is provided within the deadline by the enforcing state, the data can be transferred. During legislative negotiations, a compromise was found based on a differentiation between 'domestic' and 'non-domestic' cases. The agreed system provides for direct orders without notification for all preservation orders, production orders for all subscriber data and data for the sole purpose of identifying the user, as well as for production orders for traffic and content data if the case is considered 'domestic'. If it is considered 'non-domestic', a notification procedure is introduced for traffic and content data with a ten-day objection

⁷⁶ Ibid., Arts. 10 and 11. The initial Commission proposal included also a refusal by the provider of an order that manifestly violates the EU Charter or is manifestly abusive (Art. 9(5), second subparagraph, of the initial Commission proposal (see footnote 60)). This was deleted due to criticism that service providers should not make fundamental rights assessments. However, it seems tacitly still existing as the enforcing authority can refuse the enforcement based on a similar fundamental rights ground based on Article 6 of the Treaty on European Union (TEU). Consequently, the provider can raise it at the enforcement phase (E-evidence Regulation, Art. 16(3)(a)).

⁷⁷ E-evidence Regulation, Art. 16.

⁷⁸ Ibid., Art. 17.

⁷⁹ Council of the European Union, General Approach on Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters (Council General Approach), [2018] 15292/18, 12 December 2018.

⁸⁰ E-evidence Regulation, Art. 2(2).

⁸¹ Council General Approach, Art. 5(7).

⁸² Ibid., Art. 7a.

⁸³ European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee), Draft Report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, [2019] PR191404EN, 24 October 2019; LIBE Committee, Report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, [2019] A9-0256/2020, 11 December 2020.

possibility by the enforcing state on specific non-recognition grounds. The list is shorter than in the EIO Directive and includes immunities and privileges, a fundamental rights non-recognition ground based on Article 6 of the Treaty on European Union (TEU),⁸⁴ *ne bis in idem* and lack of double criminality outside the traditional list of thirty-two offences to which double criminality does not apply.⁸⁵ The two co-legislators had substantial difficulties in defining what is ‘domestic’. Under the final agreement, a case is considered ‘domestic’ if there are, at the time of issuing the order, reasonable grounds to believe that: (a) the offence has been committed, is being committed or is likely to be committed in the issuing state, and (b) the person whose data is requested resides in the issuing state. However, the Regulation does not provide a clear answer on residence. Only certain examples are provided in the recitals such as a registration, residence permit, identity card, as well as ‘certain connections with that state which are of similar degree as those resulting from establishing a formal residence’ (e.g. family ties, economic connections, a registered vehicle, a bank account). In addition, it is stated that a short visit, a holiday stay, including a holiday home, or a similar stay is not enough to establish a residence.⁸⁶ In applying the system, one of the main questions might be what to consider as ‘residence’. The term should have an autonomous meaning under EU law. The European Parliament proposed a link with Directive 2004/38/EU⁸⁷ on free movement but was rejected. Further, in emergency cases – even in ‘non-domestic’ cases where a notification is necessary – the data is transferred immediately. The enforcing authority has only an *ex post facto* opportunity (within ninety-six hours) to challenge the order and limit the use of the data transferred.⁸⁸

Consequently, in most cases under the new system, a direct transfer without notification will take place. However, this raises a number of legal issues. For a start, it is based on an extensive understanding of the legal basis (Article 82 TFEU) which requires traditionally two judicial authorities in the issuing and executing states. There is also a significant difference in scope between the Directive and the Regulation. The e-evidence Directive allows for a wider use of the legal representative, including for other instruments. Further, the system does not take into account the territorial obligations of the executing/enforcing state under the European Convention on Human Rights (ECHR). Two particular issues are the lack of judicial control in the enforcing state and extraterritoriality. This qualitatively changes current mutual recognition between judicial authorities to a system of ‘Europeanisation’ of national orders, namely a direct application of a national order across the EU. Such an approach provides for more integration, on one side, but bears the danger of the spread of common lowest denominators, on the other side. Ignoring higher national standards for accessing certain data (e.g. court orders for IP addresses) by the e-evidence Regulation is an indicator of that. The issue will be analysed in more detail in Section 1.4.

⁸⁴ The fundamental rights non-recognition ground is a hybrid between Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders, [2018] OJ L 303, 28 November 2018, p. 1, and the EIO Directive. It uses the more limited terms from the mentioned Regulation but a reference to Article 6 TEU from the mentioned Directive. It reads: ‘in exceptional situations, there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution order would, in the particular circumstance of the case, entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and the Charter’.

⁸⁵ See, e.g., e-evidence Regulation, Art. 12.

⁸⁶ Ibid., Recital 53. See also Case C-66/08, *Kozłowski* [2008] ECLI:EU:C:2008:437, on the reference for ‘staying’.

⁸⁷ Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No. 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC, [2004] OJ L 158, 30 April 2004, p. 77.

⁸⁸ E-evidence Regulation, Art. 3, point 18 (definition of ‘emergency case’) and Arts. 10(4) and 12.

1.2.3.2 Terrorist Content Online

Regulation (EU) 2021/784⁸⁹ prescribes obligations for private providers and member states in view of terrorist content online. It introduces a one-hour deadline for the hosting service provider to react on national removal orders,⁹⁰ provides for direct cross-border removal orders,⁹¹ prescribes proactive obligations for certain providers⁹² and defines cooperation between service providers, competent authorities and Europol.⁹³ There is no court order requirement for the removal, as competent authorities can be also administrative ones.⁹⁴ It also introduces, similar to the e-evidence logic, extraterritorial application as it applies to hosting service providers ‘offering services in the Union, irrespective of their place of main establishment’, insofar as they disseminate information to the public.⁹⁵ Such a provider has to designate a legal representative in the Union for the purpose of the TCO (terrorist content online) Regulation.

In comparison with the initial Commission proposal, the final text provides a higher level of legal certainty. However, not all points of criticism were tackled.⁹⁶ For example, the notion of terrorist content online is explicitly connected with Directive (EU) 2017/541.⁹⁷ This solves the issue only partially due to the problematic nature of certain provisions of that Directive itself in view of legal clarity (foreseeability) and legality.⁹⁸ The issue has been raised by UN experts,

⁸⁹ Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (TCO Regulation), [2021] OJ L 172, 17 February 2021, p. 79.

⁹⁰ TCO Regulation, Art. 3.

⁹¹ Ibid., Art. 4. A notification is sent simultaneously to the provider and the member state where the provider is established or its representative resides. The other state can react on its own or upon the notice of the hosting service provider or content provider (made within forty-eight hours) in a deadline of seventy-two hours. It adopts a reasoned decision if the order seriously or manifestly infringes the Regulation or fundamental rights and freedoms from the Charter. However, during that time the content is in principle removed or disabled.

⁹² Ibid., Art. 5 on specific measures to be taken by an exposed provider. Such measures could include proactive technical screening (voluntary upload filters). See also Recital 25 stating that ‘it should be possible for hosting service providers to use automated tools if they consider this to be appropriate and necessary to effectively address the misuse of their services for the dissemination of terrorist content’. Automated tools for screening are mentioned also in Art. 7(1) on safeguards. To be considered as an exposed provider, two final removal orders in twelve months are enough (Art. 5(4)).

⁹³ TCO Regulation, Art. 14.

⁹⁴ Ibid., Arts. 12 and 13 on definition of ‘competent authorities’. They should only ‘carry out their tasks . . . in an objective and non-discriminatory manner while fully respecting fundamental rights’. See also Recital 35.

⁹⁵ TCO Regulation, Arts. 1(2), 16 and 17.

⁹⁶ See, e.g., Diego Naranjo, ‘Antiterrorists in a Bike Shed – Policy and Politics of the Terrorist Content Regulation’, *EDRi*, 25 May 2021, <https://edri.org/our-work/antiterrorists-in-a-bike-shed-policy-and-politics-of-the-terrorist-content-regulation/> stating that ‘an ill-fated law with dubious evidence base, targeting an important modern problem with poorly chosen measures, goes through an exhausting legislative process to be adopted without proper democratic scrutiny due to a procedural peculiarity’. See also Chloé Berthélémy, ‘Terrorist Content Online: Is This the End?’, *EDRi*, 16 December 2020, <https://edri.org/our-work/terrorist-content-online-is-this-the-end/> assessing the positive and negative sides of the reached compromise.

⁹⁷ Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, [2017] OJ L 88, 31 March 2017, p. 6. In comparison, European Commission, Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online, [2018] (COM(2018)640 final), 12 September 2018 left the term open. See also Art. 1(3) and Recital 12 TCO Regulation stating that material for educational, journalistic, artistic, research or preventive purposes, ‘including material which represents an expression of polemic or controversial views in the course of public debate’, shall not be considered terrorist content.

⁹⁸ For example, Directive (EU) 2017/541, Art. 5 (public provocation to commit a terrorist offence), Art. 9 (travelling for the purpose of terrorism) and Art. 10 (organising or otherwise facilitating travelling for the purpose of terrorism). See the joint statement by Amnesty International, the European Network Against Racism (ENAR), European Digital

together with points on content moderation policies and the cross-border mechanism.⁹⁹ At the same time, it still allows police and administrative orders, hence orders from authorities that are not independent and impartial.¹⁰⁰ In view of the Commission's plan to address other forms of illegal content,¹⁰¹ such a mechanism could become a model for the removal or blocking of other content.

1.2.3.3 Temporary Derogation from e-Privacy for Combating Online Child Sexual Abuse

Regulation (EU) 2021/1232¹⁰² provides for a temporal derogation (till 3 August 2024) from e-privacy rules, namely Articles 5(1) and 6(1) of Directive 2002/58/EC (ePrivacy Directive).¹⁰³ The mentioned articles refer to confidentiality of communication, and erasure and anonymisation of traffic data. Such obligations can be disregarded if an exception according to Article 15(1) of Directive 2002/58/EC exists. Any exception must be provided by law and must be necessary, appropriate and proportionate within a democratic society to safeguard national security (state security), defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. In addition, such limitations have to be in line with Article 6 TEU in view of fundamental rights. The Commission justified its proposal by the application of the European Electronic Communications Code,¹⁰⁴ which covers so-called number-independent interpersonal communications services. It stated:

The ePrivacy Directive does not contain an explicit legal basis for voluntary processing of content or traffic data for the purpose of detecting child sexual abuse online. Therefore, for the services falling within scope of the ePrivacy Directive, providers will be able to continue to apply such measures only if Member States adopt legislative measures justified on the grounds laid down in Article 15 of that Directive and meeting the requirements of that provision.¹⁰⁵

Rights (EDRi), the Fundamental Rights European Experts (FREE) Group, Human Rights Watch, the International Commission of Jurists (ICJ) and the Open Society Foundations (OSF), 'European Union Directive on Counterterrorism Is Seriously Flawed', 30 November 2016, www.enar-eu.org/european-union-directive-on-counterterrorism-is-seriously-flawed-1251/.

⁹⁹ See United Nations, Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the right to privacy; and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, [2018]OL OTH 71/2018, 7 December 2018, <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gld=24234>.

¹⁰⁰ The EU legislator did not follow the UN recommendation on that. The published list by the Commission of designated authorities shows that they are mostly police authorities. See European Commission, List of national competent authority (authorities) and contact points, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en.

¹⁰¹ See Communication from the Commission to the European Parliament and the Council, A more inclusive and protective Europe: Extending the list of EU crimes to hate speech and hate crime, [2021] (COM/2021/777 final), 9 December 2021.

¹⁰² Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, [2021] OJ L 274, 30 July 2021, p. 41.

¹⁰³ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, [2002] OJ L 201, 31 July 2002, p. 37.

¹⁰⁴ Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, [2018] OJ L 321, 17 December 2018, p. 36.

¹⁰⁵ European Commission, Proposal for the Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the

While acknowledging that such measures constitute an interference with fundamental rights,¹⁰⁶ the EU legislator nevertheless provided parameters under which an interference is justified. They include necessity and proportionality, data protection by design and default as regards the technology used, a prior impact assessment and consultation in line with Articles 35 and 36 GDPR, reliability of technology, time limitation of storage (up to twelve months) and specific obligations for providers (redress, human intervention, clear information of users, reporting obligations and so on).¹⁰⁷

The introduced system covers child pornography as well as child solicitation as defined in Directive 2011/93/EU.¹⁰⁸ There is no doubt that the fight against such offences is important. However, the Regulation raises questions in view of legalising ‘client-side scanning’ (end-point filtering) whereby each sent message is first checked against a database of ‘hashes’, or unique digital fingerprints, usually of images or videos. If there is a match, the system may refuse to send your message, notify the recipient or forward it to a third party. This means that encryption is disabled and content not private. The use of such technology is compared with the logic of digital dog sniff based on a hit/no hit basis. Therefore, it is claimed that the intrusion into privacy is limited.¹⁰⁹ However, even the voluntary policies of some providers (based on their terms of service) were disputed in courts, although mainly on the question of providers acting as government agents.¹¹⁰ The issue becomes more problematic in view of new technology beyond the ‘hash’ technique. The latter provides only a binary result (hit/no hit). Newer technologies include probabilistic assessments with AI.¹¹¹ In view of the possible intrusiveness of such measures, a comprehensive public and legislative debate would be necessary. The political connotation and speed under which the Regulation was adopted puts this into question. It is also illusionary that such tools, once introduced, will be used only for combating child sexual abuse. An extension to other forms of illegal conduct is likely (terrorism, hate speech, drugs and so on).¹¹² Giving legislative permission to private providers to use such technology transforms them into state agents. However, invasive digital searches should be allowed only to law enforcement authorities by specific warrants and prior suspicion. The matter becomes even more important as the intention is

processing of personal and other data for the purpose of combatting child sexual abuse online, [2020] (COM(2020) 568 final), 10 September 2020.

¹⁰⁶ Regulation (EU) 2021/1232, Recitals 8 to 10.

¹⁰⁷ Ibid., Art. 3.

¹⁰⁸ Directive 2011/93/EU, p. 1.

¹⁰⁹ See E. Portnoy, ‘Why Adding Client-Side Scanning Breaks End-to-End Encryption’, *Electronic Frontier Foundation*, 1 November 2019, www.eff.org/uk/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption; Y. Grauer, ‘Why Email Providers Scan Your Emails’, *Consumer Reports*, 2 July 2021, www.consumerreports.org/privacy/why-email-providers-scan-your-emails-a8433077582/.

¹¹⁰ See D. Martin, ‘Demystifying Hash Searches’ (2018) 70 *Stanford Law Review* 693–733. The author claims that such techniques can violate the Fourth Amendment on the prohibition of unreasonable searches and seizures and are similar to historically prohibited general warrants. See also *U.S. v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009):

For example, the government has sophisticated hashing tools at its disposal that allow the identification of well-known illegal files (such as child pornography) without actually opening the files themselves. These and similar search tools may not be used without specific authorization in the warrant, and such permission may only be given if there is probable cause to believe that such files can be found on the electronic medium to be seized.

¹¹¹ See Martin, ‘Demystifying Hash Searches’, 722–727.

¹¹² The extension from ‘hash’ technology to more invasive technologies is acknowledged in Recital 7 stating that ‘[t]he technology used for those activities could be hashing technology for images and videos and classifiers and artificial intelligence for analysing text or traffic data’. History teaches us that exceptions have a tendency to become a rule. For example, the inquisitorial criminal procedure in continental Europe was intended only for the most serious religious offences but became a model for all offences for several hundred years. See A. Esmein, *A History of Continental Criminal Procedure: With Special Reference to France* (Boston: Little, Brown and Company, 1913), 78–144.

to replace the interim Regulation with a permanent one¹¹³ imposing an obligation for online service providers to use such techniques.¹¹⁴

Consequently, all mentioned instruments show as a common trend an increased, kind of ‘state agent’ role in crime prevention for private providers. In view of the secrecy of the measures applied, it will be also mainly them who will have the effective possibility to oppose such measures. However, through this we are putting them into a schizophrenic position to promise respect of privacy and data protection as business models to customers, and at the same time ‘control’ their customers for possible illegal behaviour for the government. The mentioned instruments (many adopted under the legal basis of Article 114 TFEU on the internal market) also raise the question of the understanding of privacy in modern technological societies that consider themselves democracies.

1.3 THE RIGHT TO PRIVACY AS THE NEW MAIN FUNDAMENTAL RIGHT

Classically, the right to life and the right to liberty were the main fundamental rights in view of intrusiveness in the case of their violation, followed by the prohibition against torture. This is reflected, for example, in the absolute nature of Article 2 (together with Protocols 6 and 13) and Article 3 ECHR,¹¹⁵ and the strict requirements for limitations of the right to liberty and security under Article 5 ECHR. The right to privacy for a long time did not exist as such and was not explicitly mentioned in several constitutions.¹¹⁶ Only certain aspects of the right to privacy were considered and taken into account, mainly its territorial aspect, referring to the sanctity of one’s home. It was gradually developed from the notion of the right to life and liberty, and civil privileges, while the term ‘property’ was extended to include all kinds of possession, tangible and intangible.¹¹⁷

¹¹³ Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, [2022] (COM/2022/209 final), 11 May 2022. A national coordinating authority could request from a national judicial or independent administrative authority to issue an order and force the provider to install and operate such technologies (Art. 10). Whereby the assessment of the judicial or independent administrative authority seems limited as it ‘shall’ issue the order if: (a) there is evidence of a significant risk of the service being used for the purpose of online child sexual abuse, and (b) the reasons for issuing the detection order outweigh negative consequences for the rights and legitimate interests of all parties affected, having regard in particular to the need to ensure a fair balance between the fundamental rights of those parties (Art. 7(4)). See also LIBE Committee, Draft Report on the proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, [2023] PR177026EN, 19 April 2023.

¹¹⁴ See, e.g., EDRI, ‘European Commission’s Online CSAM Proposal Fails to Find Right Solutions to Tackle Child Sexual Abuse’, EDRI, 11 May 2022, <https://edri.org/our-work/european-commissions-online-csam-proposal-fails-to-find-right-solutions-to-tackle-child-sexual-abuse/>. See also the negative opinion on the proposal by the Legal Service of the Council of the European Union, [2023] 8787/23, 26 April 2023. It stated that the envisaged system is not being sufficiently clear, precise and complete and, therefore, is not in compliance with the requirement that the limitations to fundamental rights must be provided for by law. And it is not proportionate in view of the general and indiscriminate screening of the data and its application, without distinction, to all the persons using that specific service, without them being, even indirectly, in a situation liable to give rise to criminal prosecution.

¹¹⁵ Prohibition of derogation under Art. 15(2) of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), 4 November 1950.

¹¹⁶ For example, the Indian Supreme Court declared privacy an existing right only in 2017. In the case of Justice K. S., Puttuswamy (Retd.) and Another v. Union of India and Others, No. 494/2012, 24 August 2017, relating to the introduction of a national identification card with biometric data allowing the tracking of a persons, it stated that it is a fundamental right derived from Arts. 14, 19 and 21 of the Indian Constitution, namely equality before the law, freedom of expression and right to life and liberty.

¹¹⁷ S. D. Warren and L. D. Brandeis (1890) 4(5) ‘The Right to Privacy’, *Harvard Law Review* 193–220. The authors stated:

The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise

So, privacy started to be considered more broadly, as a specific ‘right to be let alone’,¹¹⁸ and, if not provided explicitly in constitutions, as a natural right combining aspects of several other rights – the ‘penumbra doctrine’.¹¹⁹ It became a broader right in the last decades, including aspects of personal dignity,¹²⁰ sexual orientation,¹²¹ family¹²² and so on. It started being analysed from specific viewpoints, such as those relating to its territorial or communication aspects, and certain independent rights, like data protection, developed from it.¹²³ Further, modern technology in the last decades changed its meaning substantially. Today, permanent surveillance of one’s life is possible without the necessity of physical restraint or breaking into one’s premises. Everything can be gathered with a ‘click of a button’. Consequently, the role of privacy has to be reassessed. Some claim that such a right is obsolete and will not survive, while others consider it essential to keep technology within certain boundaries, to allow a ‘right to be let alone’ also in the digital age.¹²⁴ To understand the issue better, a short overview of the origins and changes in the concept of privacy will be provided, looking at, for example, US Supreme Court and ECtHR case law in view of modern digital surveillance.

1.3.1 *From a Property Concept of Privacy to the Right to Be Let Alone*

The right to privacy was initially a right associated with one’s property and home, and as such recognised in the English legal system in the eighteenth century. It was connected with trespass, illegal home searches and seizures of documents (‘my home is my castle’). One of the first

and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.

¹¹⁸ The term was first used by T. Cooley, *Treatise on the Law of Torts* (Chicago, IL: Callaghan and Company, 1888). See also D. J. Glancy, ‘The Invention of the Right to Privacy’ (1979) 21(1) *Arizona Law Review* 1–39.

¹¹⁹ The penumbra theory proclaims that several amendments of the Bill of Rights cast a ‘penumbra’ (shadow) and create together the right to privacy, although not explicitly mentioned in the US Constitution and Bill of Rights. It was first used by the US Supreme Court in *Griswold v. Connecticut*, 381 US 479 (1965), on the illegality to provide birth control counselling to a married couple. The court stated that

specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. . . . Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one The Third Amendment, in its prohibition against the quartering of soldiers “in any house” in time of peace without the consent of the owner, is another facet of that privacy. The Fourth Amendment explicitly affirms the “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” The Fifth Amendment, in its Self-Incrimination Clause, enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

In later US Supreme Court cases it was connected with substantive due process, for example in *Roe v. Wade*, 410 US 113 (1973), overturned by *Dobbs v. Jackson Women’s Health Organization*, 597 US (2022).

¹²⁰ *Pfeifer v. Austria*, Appl. No. 12556/03, 15 November 2007, para. 35; *Denisov v. Ukraine*, Appl. No. 76639/11, 25 September 2018, paras. 97–99; *Beizaras and Levickas v. Lithuania*, Appl. No. 41288/15, 14 January 2020, para. 117; and so on.

¹²¹ *Dudgeon v. United Kingdom*, Appl. No. 7527/76, 22 October 1981, paras. 40–41; *Orlandi and Others v. Italy*, Appl. Nos. 26431/12, 26742/12, 44057/12 and 60088/12, 14 December 2017.

¹²² *Slivenko v. Latvia*, Appl. No. 48321/99, 9 October 2003, para. 97; *Şerife Yiğit v. Turkey*, Appl. No. 3976/05, 2 November 2010; *Vavříčka and Others v. Czech Republic*, Appl. No. 47621/13, 8 April 2021, para. 264.

¹²³ See in detail Chapter 3 on data protection in this volume.

¹²⁴ See N. Richards, *Why Privacy Matters* (Oxford: Oxford University Press, 2021), 35–69; A. W. Geiger, ‘How Americans Have Viewed Government Surveillance and Privacy since Snowden Leaks’, *Pew Research Center*, 4 June 2018, www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/.

English cases illustrating this is *Entick v. Carrington*,¹²⁵ where, upon an administrative order, agents entered Entick's private home, searched it for hours and seized a variety of documents in connection with an accusation of seditious libel against the King's government; they also arrested Entick. At a tort trial (damages), the court found for the plaintiff,¹²⁶ limiting intrusions only to those allowed by legislation or common law. The court concluded that the State Secretary that had issued the warrant could not be considered a 'conservator of peace' (similar to a justice of the peace) and had beyond the offence of high treason no power to issue such warrants. Therefore, the officers were not within the equity of the Constables Protection Act, special legislation that provided impunity for actions of officers based on legal warrants.¹²⁷

The case has had a significant impact on the Fourth Amendment of the Bill of Rights¹²⁸ to the US Constitution protecting people from unreasonable searches and seizures, as well as on the Fifth Amendment's privilege against self-incrimination. It was understood that both Amendments form a zone of privacy.¹²⁹ With the start of modern telecommunication technology from the 1920s onwards (first, with the possibility of wiretapping and recording of classical telephone conversations), the concept of privacy had to be substantially transformed – from an 'ownership/property' concept based on trespass to an 'expectation of privacy' concept. This can be illustrated by comparing the US Supreme Court cases *Olmstead et al. v. United States*¹³⁰ and *Katz v. United*

¹²⁵ *Entick v. Carrington and three other Messengers in ordinary to the King* [1765] EWHC KB J98. The case was part of a broader political conflict (criticism of the British government for concluding peace with France regarding the Seven Years' War and the connected Wilkes case regarding libel against the king) and the issue of use of general warrants without determining a specific suspect in advance. In the mentioned case, the jury addressed a question to the court to determine if the search was illegal, which the court confirmed. See T. Hickman, 'Revisiting Entick v Carrington: Seditious Libel and State Security Laws in Eighteenth-Century England', in A. Tomkins and P. Scott (eds.), *Entick v Carrington, 250 Years of the Rule of Law* (Oxford: Hart, 2015), 42–84. For a modern comparison, see the CJEU judgment in the *EncroChat* case, where the court did not see any issue with the indiscriminate interception of telecommunications, regardless of the non-existence of prior individual suspicion. The court concluded that Article 6(1) of the EIO must be interpreted as not precluding a public prosecutor from issuing an EIO for the transmission of evidence already in the possession of the competent authorities of the executing state where that evidence has been acquired following the interception, by those authorities, on the territory of the issuing state, of telecommunications of all the users of mobile phones which, through special software and modified hardware, enable end-to-end encrypted communication, provided that the EIO satisfies all the conditions that may be laid down by the national law of the issuing state for the transmission of such evidence in a purely domestic situation in that state. Case C-670/22, MN [2024] ECLI:EU:C:2024:372.

¹²⁶ He did not issue proceedings for unlawful arrest to influence the choice of court.

¹²⁷ There is controversy about the exact statements by Lord Camden in view of the absence of official records. See T. T. Arvind and C. R. Burset, 'A New Report of Entick v. Carrington (1765)' (2022) 110(1) *Kentucky Law Journal* 265–232.

¹²⁸ Fourth Amendment: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

¹²⁹ See also *Boyd v. United States*, 116 US 616 (1886), where the court declared as unconstitutional a law requiring in revenue cases, on motion from the government attorney, a person to produce in court his private books, invoices and papers, or else the allegations of the attorney to be taken as confessed and goods forfeit. The court stated:

It is not the breaking of his doors and the rummaging of his drawers that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property . . . Breaking into a house and opening boxes and drawers are circumstances of aggravation, but any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods is within the condemnation of that judgment. In this regard, the Fourth and Fifth Amendments run almost into each other.

See also Michigan Law Review, "The Life and Times of *Boyd v. United States* (1886–1976)" (1977) 76(1) *Michigan Law Review* 184–212.

¹³⁰ *Olmstead et al. v. United States*, 277 US 438 (1928). The case included several instances of wiretappings as regards bootlegging (illegal production and sale of alcohol). See also *Goldman v. United States*, 316 US 129 (1942) – The use by federal agents of a detectaphone, whereby conversations in the office of a defendant were overheard through contact on the wall of an adjoining room, did not violate the Fourth Amendment, and obtained evidence was admissible.

States,¹³¹ which are divided by four decades. In *Olmstead* a majority of justices (five to four) still insisted on a property concept of privacy regarding the Fourth Amendment and, hence, did not consider that wiretapping telephone conversations without entering private premises raised any constitutional issues, referring to the original meaning of the framers. In contrast, Justice Brandeis, in his prophetic dissenting opinion, discussed the right to be let alone, stating:

To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth. . . . It is, of course, immaterial where the physical connection with the telephone wires leading into the defendants' premises was made. And it is also immaterial that the intrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.¹³²

His opinion was taken up forty years later in *Katz* addressing the issue of calls intercepted from a public telephone booth used for placing illegal interstate bets. The court stated that the Fourth Amendment not only governs the seizure of tangible items but extends as well to the recording of oral statements, and that it protects people, rather than places. Therefore, its reach cannot turn on the presence or absence of a physical intrusion into any given enclosure. As a consequence, it explicitly overturned the 'trespass' doctrine from *Olmstead* and *Goldman*.¹³³ At the same time it acknowledged that such an intrusion should be authorised by a court warrant.¹³⁴ It was the concurring opinion of Justice Harlan that introduced the term 'reasonable expectation of privacy', namely, it is unconstitutional under the Fourth Amendment without a warrant to conduct a search and seizure anywhere that a person has a reasonable expectation of privacy. In *Smith v. Mariland*,¹³⁵ a twofold requirement was confirmed: first, a person must have exhibited an actual (subjective) expectation of privacy and, second, the expectation should be one that society is prepared to recognise as 'reasonable'.¹³⁶ This double test became an intrinsic part of the Fourth Amendment,¹³⁷ although later additional aspects were added to take into account the interest of law enforcement. For example, a 'third-party' doctrine has been developed on

¹³¹ *Katz v. United States*, 389 US 347 (1967).

¹³² He warned that illegal wiretappings were a crime and stated:

Our Government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the Government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that, in the administration of the criminal law, the end justifies the means – to declare that the Government may commit crimes in order to secure the conviction of a private criminal – would bring terrible retribution.

¹³³ *Olmstead et al. v. United States*; *Goldman v. United States*.

¹³⁴ The court evaluated several exceptions (search incident to arrest, hot pursuit or consent), finding that none applied, and declined the creation of a new one. However, the majority refused to answer on whether the same rules would apply in cases of national security.

¹³⁵ *Smith v. Mariland*, 42 US 735 (1979). Installation and use of a pen register does not constitute a violation of the suspect's reasonable expectation of privacy since the telephone numbers would be available to and recorded by the phone company.

¹³⁶ Justice Black dissented and compared wiretapping to eavesdropping as well as denying a constitutional standing to privacy.

¹³⁷ *Mancusi v. DeForte*, 392 US 364 (1968). See also N. Strossen, 'Justice Harlan's Enduring Importance for Current Civil Liberties Issues, from Marriage Equality to Dragnet NSA Surveillance' (2017) 61(3) *New York Law School Law Review* 331–345.

the lawfulness of information that a person provides voluntarily to others. In addition, a set of exceptions was recognised in view of warrantless searches, such as search incident to a lawful arrest,¹³⁸ stop and frisk,¹³⁹ plain view,¹⁴⁰ consent,¹⁴¹ good faith¹⁴² and so on.¹⁴³ Such doctrines are also being applied to the modern digital world.

1.3.2 Privacy and Certain Modern Technology Issues

In several cases the US Supreme Court dealt with the issue of applying the ‘reasonable expectation of privacy test’ to modern technology. For example, in *Kyllo v. United States*,¹⁴⁴ it invalidated the warrantless use of a thermal imaging device directed at a private home from a public street to check for possible growing of marijuana. It stated that ‘obtaining by sense enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical “intrusion into a constitutionally protected area,” . . . constitutes a search at least where (as here) the technology in question is not in general public use’. In *United States v. Jones*,¹⁴⁵ it held that installing a tracking Global Positioning System (GPS) device on a vehicle and using it to monitor the vehicle’s movements constitutes a search. The majority considered that it was illegal due to property concerns. And a minority referred to the reasonable expectation of privacy test. The case also indicates the so-called mosaic theory on the existence of an infringement due to the sum of intrusions (not by a single one), through certain hints in the concurring opinion of Justice Alito and even more so in the opinion of Justice Sotomayor.¹⁴⁶ In *Riley v. California*,¹⁴⁷ the Court excluded the search of cell phones from the search incident to arrest doctrine also using the expectation of privacy doctrine. The Court stated that ‘[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans “the privacies of life.” The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.’ This was

¹³⁸ *Chimel v. California*, 395 US 752 (1969); *United States v. Robinson*, 414 US 218 (1973).

¹³⁹ *Terry v. Ohio*, 392 US 1 (1968) – A police officer may stop a suspect on the street and frisk him or her without probable cause to arrest, if the police officer has a reasonable suspicion that the person has committed, is committing or is about to commit a crime and has a reasonable belief that the person may be armed and presently dangerous.

¹⁴⁰ *Coolidge v. New Hampshire*, 403 US 443 (1971). See about the use of this doctrine for computer searches – J. Saylor, ‘Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches’ (2011) 79(6) *Fordham Law Review* 2809–2858.

¹⁴¹ *Schneekloth v. Bustamonte*, 412 US 218 (1973); *Ohio v. Robinette*, 519 US 33 (1996); *United States v. Drayton*, 536 US 194 (2002).

¹⁴² *United States v. Leon*, 468 US 897 (1984).

¹⁴³ Such exceptions developed together with a reinterpretation of the Fourth Amendment’s exclusionary rule on admissibility of evidence. The reasoning went from a principled rule similar to the exclusionary rule of the Fifth Amendment in *Mapp v. Ohio*, 367 US 643 (1961) to a utilitarian rule in *U.S. v. Calandra*, 414 US 338 (1974).

¹⁴⁴ *Kyllo v. United States*, 533 US 27 (2001). It distinguished the case from *California v. Ciraolo*, 476 US 207 (1986), whereby the Court held that warrantless aerial observation of a person’s backyard did not violate the Fourth Amendment.

¹⁴⁵ *United States v. Jones*, 565 US 400 (2012). In *Jones* the Supreme Court substantially refined its approach on the understanding of the Fourth Amendment, and differentiated the case from *United States v. Knotts*, 460 US 276 (1983), regarding the warrantless use of a radio beeper for an afternoon.

¹⁴⁶ C. Slobogin, ‘Making the Most of *United States v. Jones* in a Surveillance Society: A Statutory Implementation of Mosaic Theory’ (2012) 8 *Duke Journal of Constitutional Law & Public Policy* 1–37; D. C. Grey and D. Keats Citron, ‘A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy’ (2013) 14(2) *North Carolina Journal of Law & Technology* 381–430; O. S. Kerr, ‘The Mosaic Theory of the Fourth Amendment’ (2012) 111(3) *Michigan Law Review* 311–354.

¹⁴⁷ *Riley v. California*, 573 US 373 (2014).

further elaborated in *Carpenter v. United States*,¹⁴⁸ whereby the Court limited the third-party doctrine in the case of cell site location information (CSLI) meaning that a court warrant was necessary to get the data from the provider. It considered that such data is at the crossroads between GPS tracking requiring a warrant and the warrantless third-party doctrine (data given voluntarily to the provider). However, it tilted the balance based on an expectation of privacy test against the government, stating:

Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations." . . . These location records "hold for many Americans the privacies of life." . . . And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.

Such cases and others show the usefulness of the expectation of privacy concept in modern technological society. The issue with such technology is no longer about a physical intrusion into one's home; it is about governmental self-restraint in view of the technology used based on objectively acknowledged spheres of the individual's privacy.¹⁴⁹

1.3.3 *The ECtHR on the Reasonable Expectation of Privacy*

The same issues as debated in the United States are also part of the European debate on protection of fundamental rights. The ECHR has in Article 8 an explicit and broad definition of privacy that specifically mentions respect for private and family life, home and correspondence. The ECtHR has stated several times that it is not possible to provide an exhaustive definition of privacy. It covers physical and psychological integrity, as well as the right to develop relationships with others (private social life). The ECtHR is also using the 'reasonable expectation(s) of privacy' concept developed by the US Supreme Court.¹⁵⁰

The first time it used the term was in *Halford v. United Kingdom*¹⁵¹ on the use of an office phone for private conversations. The Court stated:

There is no evidence of any warning having been given to Ms Halford, as a user of the internal telecommunications system operated at the Merseyside police headquarters, that calls made on that system would be liable to interception. She would . . . have had a reasonable expectation of privacy for such calls, which expectation was moreover reinforced by a number of factors. As Assistant Chief Constable she had sole use of her office where there were two telephones, one of which was specifically designated for her private use. Furthermore, she had been given the

¹⁴⁸ *Carpenter v. United States*, 585 US (2018). See, e.g., E. Park, 'Objects, Places and Cyber-Spaces Post-Carpenter: Extending the Third-Party Doctrine Beyond CSLI – A Consideration of Internet of Things (IoT) and DNA' (2019) 21(1) *Yale Journal of Law & Technology* 1–57.

¹⁴⁹ The warrantless third-party doctrine was refused in view of the National Security Agency's (NSA) metadata collection programme in the United States. See, e.g., Electronic Privacy Information Center (EPIC), 'Appeals Court: NSA Call Metadata Program Was Illegal, Likely Unconstitutional', EPIC, 2 September 2020, <https://epic.org/appeals-court-nsa-call-metadata-program-was-illegal-likely-unconstitutional/>.

¹⁵⁰ The Court sometimes uses 'reasonable expectation of privacy' and sometimes only 'expectation of privacy'.

¹⁵¹ *Halford v. United Kingdom*, Appl. No. 20605/92, 25 June 1997. Ms Halford alleged that members of the Merseyside Police Authority intercepted office telephone calls in response to a complaint to the Industrial Tribunal due to refusals to promote her to a higher position based on her sex.

assurance, in response to a memorandum, that she could use her office telephones for the purposes of her sex-discrimination case.’

The concept has been referred to in other cases on privacy in the working place,¹⁵² as well as in cases on balance between freedom of expression (Article 10 ECHR) and privacy.¹⁵³ However, in *Benedik*,¹⁵⁴ the Court used the doctrine specifically on IP addresses and the internet. It stated that ‘the question is clearly not whether the applicant could have reasonably expected to keep his dynamic IP address private but whether he could have reasonably expected privacy in relation to his identity’, and further that

[the] anonymity conception of privacy is an important factor to be taken into account in the present assessment. In particular, it has not been argued that the applicant had ever disclosed his identity in relation to the online activity in question . . . or that he was for example identifiable by the particular website provider through an account or contact data. His online activity therefore engaged a high degree of anonymity . . . Lastly, the Court notes that the applicable legal and regulatory framework might also be a relevant, though not necessarily decisive, factor in determining the reasonable expectation of privacy . . . As to the statutory framework, the Court finds it sufficient to note that Article 37 of the Constitution guaranteed the privacy of correspondence and of communications and required that any interference with this right be based on a court order Therefore, also from the standpoint of the legislation in force at the relevant time, the applicant’s expectation of privacy with respect to his online activity could not be said to be unwarranted or unreasonable.¹⁵⁵

For the assessment of Article 8 ECHR cases, the Court uses the concept to establish beforehand if privacy is implicated. Once this is established or if the matter clearly falls under privacy, it continues its assessment depending on the nature of the violation. In the case of an interference by the government, it uses the traditional test of Article 8(2) ECHR, namely, that the interference was provided by law, followed a legitimate goal and was necessary in a democratic society.¹⁵⁶ In the case of positive obligations by the state to interfere in relationships between individuals, it assesses if the government has set up a legislative framework taking into consideration the various interests to be protected in a particular context. This could address the sexual integrity of minors,¹⁵⁷ medical negligence¹⁵⁸ or privacy in the working place.¹⁵⁹ However, there is a significant difference in the application of the test between the US and the ECtHR systems. In the US the application of the test determines the obligation to use a warrant. In comparison, the ECtHR uses it only as an entry point to assess if privacy is affected at all. It is deplorable that the ECtHR does not necessarily require a prior court warrant once certain aspects of privacy are affected (communications or home). For example, according to ECtHR case law, absence of a prior judicial warrant for house searches in non-urgent circumstances may be counterbalanced

¹⁵² See *Peev v. Bulgaria*, Appl. No. 64209/01, 26 July 2007. A search at the office which extended to the applicant’s desk and filing cabinets amounted to an interference with private life.

¹⁵³ See *Von Hannover v. Germany*, Appl. No. 59320/00, 24 June 2004, para. 51.

¹⁵⁴ *Benedik v. Slovenia*, Appl. No. 62357/14, 24 April 2018. The applicant exchanged child abuse material over the Razorback network. Upon detection, the Swiss authorities informed the Slovenian authorities, which then obtained IP information without a court order.

¹⁵⁵ *Benedik v. Slovenia*, paras. 116–118.

¹⁵⁶ *Sorvisto v. Finland*, Appl. No. 19348/04, 13 January 2009, paras. 104–105; *Akhlyustin v. Russia*, Appl. No. 21200/05, 7 November 2017, paras. 36–39; *Uzun v. Germany*, Appl. No. 35623/05, 2 September 2010, paras. 49–53.

¹⁵⁷ *X and Y v. Netherlands*, Appl. No. 8970/80, 26 March 1985; *K.U. v. Finland*, Appl. No. 2872/02, 2 December 2008.

¹⁵⁸ *Codarcea v. Romania*, Appl. No. 31675/04, 2 June 2009.

¹⁵⁹ *Bărbulescu v. Romania [GC]*, Appl. No. 61496/08, 5 September 2017, paras. 80 and 115; *Copland v. United Kingdom*, Appl. No. 62617/00, 3 April 2007, paras. 43–44; *López Ribalda and Others*, Appl. Nos. 1874/13 and 8567/13, 17 October 2019, paras. 93–95.

by the availability of an *ex post facto* judicial review.¹⁶⁰ However, the use of such a remedy depends on the affected person and does not entail the same level of protection against arbitrariness as a general system of prior court authorisations in non-urgent cases.

Furthermore, it seems that the ECtHR assesses 'reasonability' primarily from the perspective of the individual concerned.¹⁶¹ Consequently, the assessment is much more casuistic and less foreseeable, on a case-by-case basis, and not based on the use of a general and objective social standard of an 'average citizen' as in the United States. The ECtHR also unnecessarily differentiated in the past between interception of communication¹⁶² and other secret surveillance measures in view of foreseeability and the quality of the law,¹⁶³ although it backtracked to a certain extent from this position.¹⁶⁴ However, in *Big Brother Watch*,¹⁶⁵ it adapted its test to bulk non-targeted interception by national secret services. It introduced the following criteria: the grounds on which bulk interception may be authorised; the circumstances in which an individual's communications may be intercepted; the procedure to be followed for granting authorisation; the procedures to be followed for selecting, examining and using intercept material; the precautions to be taken when communicating the material to other parties; the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed; the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance; the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.¹⁶⁶ However, a minority of judges stated that court authorisation and involvement should in principle be obligatory (rather than leaving it to only an independent authority) and that a certain level of suspicion should be defined,¹⁶⁷ and one judge even rightly pointed out that the

¹⁶⁰ *Harju v. Finland*, Appl. No. 56716/09, 15 February 2011, para. 44; *Heino v. Finland*, Appl. No. 56720/09, 15 February 2012, para. 45.

¹⁶¹ *Köpke v. Germany* (dec.), Appl. No. 420/07, 5 October 2010, on video surveillance of an employee for suspected theft. The Court stated that '[a] person's reasonable expectations as to privacy is a significant though not necessarily conclusive factor'.

¹⁶² See *Valenzuela Contreras v. Spain*, Appl. No. 27671/95, 30 July 1998, para. 46 (interception of phone) and *Weber and Saravia v. Germany* (dec.), Appl. No. 54934/00, 29 June 2006, para. 95 (strategic monitoring by the secret service), requiring that the law defines the nature of offences to give rise to interception, categories of people liable to have their telephones tapped, a limit on the duration of telephone tapping, the procedure for drawing up the summary reports containing intercepted conversations and the use and destruction of the recordings made. See, e.g., *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Appl. No. 62540/00, 28 June 2007, para. 76; *Liberty and Others v. United Kingdom*, Appl. No. 58243/00, 1 July 2008, paras. 62–63; *Iordachi and Others v. Moldova*, Appl. No. 25198/02, 10 February 2009, para. 39; *Kennedy v. United Kingdom*, Appl. No. 26839/05, 18 May 2010, para. 152; *Roman Zakharov v. Russia*, Appl. No. 47143/07, 4 December 2015, para. 231.

¹⁶³ See *Bykov v. Russia* [GC], Appl. No. 4378/02, 10 March 2009, para. 78 (recording of a private conversation by way of a radio transmitting device), stating that '[t]he degree of precision required of the "law" in this connection will depend upon the particular subject-matter'; and *Uzun v. Germany*, para. 66, stating that 'adequate and effective guarantees against abuse must exist' and that the

rather strict standards, set up and applied in the specific context of surveillance of telecommunications, are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations It will therefore apply the more general principles on adequate protection against arbitrary interference.

¹⁶⁴ *R.E. v. United Kingdom*, Appl. No. 62498/11, 27 October 2015, para. 130, stating that '[t]he Court has not, therefore, excluded the application of the principles developed in the context of interception cases in covert-surveillance cases; rather, it has suggested that the decisive factor will be the level of interference with an individual's right to respect for his or her private life and not the technical definition of that interference'.

¹⁶⁵ *Big Brother Watch and Others*, Appl. Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021.

¹⁶⁶ *Big Brother Watch and Others*, para. 361.

¹⁶⁷ *Big Brother Watch and Others*. See the joint partly concurring opinion of Judges Lemmens, Vehabović and Bošnjak.

existence of such bulk collection schemes as such should be put into question.¹⁶⁸ Although bulk data and digital evidence are not directly connected, there are some common tendencies. Firstly, there is a tendency to start to transform intelligence information directly into evidence, including intercepted electronic information into electronic evidence.¹⁶⁹ Secondly, according to the new EU e-evidence system, the cross-border transfer of certain categories of e-evidence is becoming rather automatic in view of the definition of a ‘domestic’ case and the non-involvement of the enforcing state, as well as in view of the non-involvement of a court authority in the issuing or enforcing state (e.g. for IP addresses).

In light of the above ECtHR case law on digitalisation, secret surveillance and privacy leave room for reassessment and improvement, especially on the questions of intelligence services’ prerogatives in a democracy (bulk data), extraterritorial surveillance and the obligatory involvement of judges authorising certain intrusive measures. Some of those issues, namely court authorisations and extraterritorial application of law, will be further assessed in Sections 1.4.1 and 1.4.2.

1.4 IMPACT OF (CROSS-BORDER) E-EVIDENCE GATHERING ON CRIMINAL JUSTICE: SPECIFIC ISSUES

1.4.1 *Involvement of Authorities and Court Oversight in the Enforcing State*

Classical mutual recognition in EU criminal law as introduced in Tampere in 1999¹⁷⁰ and as applied in practice since its first instrument, the European Arrest Warrant (EAW), functions on the principle of direct contact between two judicial authorities.¹⁷¹ Article 82 TFEU, as the treaty basis for mutual recognition, is based on such a classical understanding. The correct application of the legal basis is essential for the principle of conferral and the delimitation of powers between the EU and member states (Article 5 TEU). This is especially true in the sensitive area of criminal law due to its strong ties with national sovereignty and national constitutional rights.¹⁷²

¹⁶⁸ *Big Brother Watch and Others*. See the partly concurring and partly dissenting opinion of Judge Pinto de Albuquerque.

¹⁶⁹ See, e.g., A. Vaško, ‘Intelligence Information within Criminal Proceedings’ (2019) 10(3) *Law, Economics and Social Issues Review* 267–283; M. Jimeno-Bulnes, ‘The Use of Intelligence Information in Criminal Procedure: A Challenge to Defence Rights in the European and the Spanish Panorama’ (2017) 8(2) *New Journal of European Criminal Law* 171–191; A. Božinovski, ‘Admissibility of (Counter-)Intelligence Information as Evidence in Court’, Geneva Centre for Security Sector Governance, 14 December 2021, www.dcaf.ch/admissibility-counter-intelligence-information-evidence-court.

¹⁷⁰ European Council, Presidency conclusions, *Towards a Union of Freedom, Security and Justice: The Tampere Milestones*, 15–16 October 1999, paras. 33–37.

¹⁷¹ Council Framework Decision 2002/584/JHA on the European Arrest Warrant and the surrender procedures between Member States (EAW Framework Decision), [2002] OJ L 190, 18 July 2002, p. 1, Art. 9(1), as amended by Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial, [2009] OJ L 81, 27 March 2009, p. 24; EIO Directive, Arts. 7(1) and (2); see Regulation (EU) 2018/1805, Arts. 4(1) and 14(1).

¹⁷² LIBE Committee, 2nd Working Document on the Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (2018/0108 (COD)) – Scope of Application and Relation with Other Instruments, [2019] DT\1176230EN, 6 February 2019. See also S. Miettinen, ‘Criminal Competence and the Choice of Legal Basis: Space in the Margins?’ (2015) 2 *European Criminal Law Review* 222–242; E. Herlin-Karnell, ‘EU Competence in Criminal Law after Lisbon’, in A. Biondi, P. Eeckhout and S. Ripley (eds.), *EU Law after Lisbon* (Oxford: Oxford University Press, 2012). See also in that regard the European Convention, *Final Report of Working Group X ‘Freedom, Security and Justice’*, [2002] CONV 426/02, 2 December 2002. The mentioned group created the basic text of the current Article 82 TFEU (Article III-270 of the never ratified Constitutional Treaty). In its final report it stated that former

Any interpretation of legal basis should not alter the Treaties.¹⁷³ Article 82(1) TFEU provides the possibility of adopting directives/regulations for the following: (a) laying down rules and procedures for ensuring recognition throughout the Union of all forms of judgments and judicial decisions; (b) preventing and settling conflicts of jurisdictions between member states; (c) supporting the training of the judiciary and judicial staff; and (d) facilitating cooperation between judicial or equivalent authorities of the member states in relation to proceedings in criminal matters and the enforcement of decisions. The e-evidence Regulation is based on Article 82(1), without specifying which of the points applies. Logically this would be points (a) and (d). Although each instrument must be evaluated by itself, past instruments can certainly be of help. Previously adopted instruments involve two judicial authorities.¹⁷⁴

Further, on the Passenger Name Record (PNR) EU–Canada Agreement,¹⁷⁵ the Court of Justice of the European Union (CJEU) followed the opinion of Advocate General Mengozzi that Article 82 TFEU is not the appropriate legal basis for a system where a private provider sends data to a law enforcement authority in a third country.¹⁷⁶ The Advocate General stated that

it is only if the Court were to adopt a more generous interpretation of Article 82(1)(d) TFEU, together, where appropriate, with Article 67(3) TFEU, which provides that the Union is to ‘endeavour to ensure a high level of security ... through measures for coordination and cooperation between police and judicial authorities and other competent authorities’, or if the contracting parties were to amend the terms of the agreement envisaged in such a way that the judicial dimension of the agreement envisaged were taken more directly into account, that Article 82(1)(d) TFEU might genuinely constitute an additional legal basis for the act concluding that agreement.¹⁷⁷

The Commission acknowledged that the e-Evidence Regulation is no longer based on this. It stated that ‘the mutual recognition principle is pushed one step further to the extent that, in the

Articles 30 and 31 TEU on police cooperation and criminal law were too vague. See also German Federal Constitutional Court, 30 June 2009, BVerfG 2 BvE 2/08, para. 253 (so-called Lisbon Treaty Judgment), stating on EU competences in criminal law that ‘particularly the newly conferred competences in the areas of judicial cooperation in criminal matters ... can, and must, be exercised by the institutions of the European Union in such a way that at Member State level, tasks of sufficient weight in extent as well as substance remain which are the legal and practical conditions of a living democracy’.

¹⁷³ See Joined Cases C-14/15 and C-116/15, *Parliament v. Council* [2016] EU:C:2016:715, para. 47, stating that ‘the Treaties alone may, in particular cases, empower an institution to amend a decision-making procedure established by the Treaties’. See also Opinion 2/94, Accession by the Community to the European Convention for the Protection of Human Rights and Fundamental Freedoms [1996] EU:C:1996:140; and Opinion 2/13, Accession of the European Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms [2014] EU:C:2014:2454, in view of the issue when a Treaty change is necessary and interpretation alone cannot solve the issue.

¹⁷⁴ For example, Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order, [2011] OJ L 338, 21 December 2011, p. 2, Art. 82(1)(a) and (d); Council Decision 2012/305/EU of 7 June 2012 on the conclusion of the Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the application of certain provisions of the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters and the 2001 Protocol thereto, [2012] OJ L 153, 14 June 2012, p. 1, Art. 82(1)(d) in conjunction with Art. 218(6)(a); Council Decision 2014/835/EU of 27 November 2014 on the conclusion of the Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the surrender procedure, [2014] OJ L 343, 28 November 2014, p. 1, Art. 82(1)(a) in conjunction with Art. 218(6)(a); EIO Directive, Art. 82(1)(a); Regulation (EU) 2018/1805, Art. 82(1)(a).

¹⁷⁵ Proposal for a Council Decision on the conclusion of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record Data, [2013] COM(2013) 528 final, 18 July 2013.

¹⁷⁶ Opinion 1/15, Transfer of Passenger Name Record Data from the European Union to Canada [2017] EU:C:2017:592, paras. 102–103.

¹⁷⁷ Opinion 1/15, Transfer of Passenger Name Record Data from the European Union to Canada, Opinion of Advocate General [2016] EU:C:2016:656, para. 108.

initial stage, there is no immediate involvement of the second Member State's judicial authorities'.¹⁷⁸ According to the Commission, a systematic involvement of the judicial authorities of the executing member state is not required under Article 82(1). Instead, it is sufficient to involve the judicial authority of the executing state should problems arise with the execution of an order by the service provider.

For the EAW, a whole set of CJEU case law was necessary to define who can be an issuing authority.¹⁷⁹ Under Article 6 of the EAW Framework Decision, the choice of issuing authority was left to the issuing member state. More recent mutual recognition instruments like the EIO Directive dealt with a similar problem relating to the definition of issuing and executing authorities. The EIO tried to keep the national system in the issuing state and at the same time to prevent lowering of national standards in the executing state. It wanted to prevent situations where authorities of a non-judicial nature (e.g. police) would order measures in another member state. judicial authorisation is not a pure technicality but goes to the core of national constitutions. For certain measures, a judicial authorisation might be a constitutional obligation. Hence, a validation procedure was introduced in the EIO Directive whereby an EIO issued by a non-judicial authority must be validated beforehand by a judge or a prosecutor, depending on national law which of the two.¹⁸⁰ This, however, did not solve the problem of the different statuses of prosecutors in different member states, with some of them having a quasi-judicial role, and being able to authorise invasive measures like house searches. The EIO clarified that procedures in the executing state 'may require a court authorisation in the executing State where provided by its national law'.¹⁸¹ This means that under the EIO system, Member State A, where the prosecutor issues an EIO, cannot directly send it for execution to Member State B if in that state a court order is necessary for the particular measure. It must be authorised beforehand by a court in Member State B, although in a more limited way than in a national case. The e-evidence system makes such a sensitive compromise obsolete.

A positive step by the e-evidence system is a court order requirement for traffic/transactional and content data, although only in the issuing state. There was consensus during legislative

¹⁷⁸ LIBE Committee, 2nd Working Document on the Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, referring to the Commission's Written Follow-Up to the European Parliament Shadows' Meeting on 9 October 2018.

¹⁷⁹ See, e.g., CJEU case law on EAW issuing authority: Case C-477/16 PPU, *Kovalkovas* [2016] ECLI:EU:C:2016:861; Case C-453/16 PPU, *Özçelik* [2016] ECLI:EU:C:2016:860; Case C-452/16 PPU, *Poltorak* [2016] ECLI:EU:C:2016:858; Joined cases C-508/18 and C-82/19 PPU, *OG and PI* [2019] ECLI:EU:C:2019:456; Case C-509/18, *PF* [2019] ECLI:EU:C:2019:457; Joined cases C-566/19 PPU and C-626/19 PPU, *JR and YC* [2019] ECLI:EU:C:2019:1077; Case C-625/19 PPU, *XD* [2019] ECLI:EU:C:2019:1078; Case C-489/19 PPU, *NJ* [2019] ECLI:EU:C:2019:849.

¹⁸⁰ See EIO Directive, Art. 2(c)(ii). The CJEU clarified that such a prosecutor does not need to be independent as required for an EAW procedure. See Case C-584/19, *A and Others* [2020] ECLI:EU:C:2020:1002. Recently, the CJEU in the *EncroChat* case reinterpreted Article 2(c) of the EIO by holding that a

European Investigation Order (EIO) for the transmission of evidence already in the possession of the competent authorities of the executing State need not necessarily be issued by a judge where, under the law of the issuing State, in a purely domestic case in that State, the initial gathering of that evidence would have had to be ordered by a judge, but a public prosecutor is competent to order the transmission of that evidence. (Case C-670/22 (see footnote 125))

¹⁸¹ EIO Directive, Art. 2(d). See A. Erbežnik, 'Mutual Recognition in EU Criminal Law and Fundamental Rights – The Necessity for a Sensitive Approach', in A. Weyembergh and C. Brière (eds.), *The Needed Balances in EU Criminal Law* (Oxford: Hart, 2018), 185–212; A. Erbežnik, 'A New EU System on Cross-Border Gathering of e-Evidence – Analysis and Open Questions' (2023) 98 *Dignitas* 47–72.

negotiations on that. However, for IP addresses or similar data for the sole purpose of identifying the person, national systems vary substantially, with a court order being required in some of them.¹⁸² To leave to member states a choice, the European Parliament opposed the creation of a new category of ‘access data’. Further, the issue of the issuing authority for such data was disputed during negotiations.¹⁸³ The European Parliament advocated for a solution used in the past in the European Evidence Warrant (EEW).¹⁸⁴ It wanted to give member states the option of making a declaration to the General Secretariat of the Council and the Commission where, in accordance with national law, the execution of an order for obtaining subscriber data and data requested for the sole purpose of identifying the user requires the procedural involvement of a court. At the end it was agreed that for IP addresses and similar indicators, no notification with a suspensive effect is required. Only a reference in a recital was added stating that ‘[w]here a notification to the enforcing authority, or enforcement, takes place in accordance with this Regulation, the enforcing State could provide under its national law that the execution of a European Production Order might require the procedural involvement of a court in the enforcing State’.¹⁸⁵ In view of the limited use of notifications to enforcing authorities in the final text (only in the case of traffic and content data when the case is considered ‘non-domestic’), data can now be collected without a court order on the territory of a member state where such an order is (constitutionally) necessary (e.g. for IP addresses). This bears the dormant danger of possible ‘Solange’ disputes similar to the *Melloni*¹⁸⁶ and *Taricco* case law.¹⁸⁷ Namely, some national constitutional courts might be requested to contradict EU law based on higher national constitutional standards on fundamental rights (requiring a court order for access to certain data).

1.4.2 Extraterritorial Application of National and EU Law

The new e-evidence approach creates new and artificial concepts of and presumptions about ‘domestic’ orders concentrating on the person and the offence, regardless of where the data is stored or where the data controller is and regardless of the territorial application of law.¹⁸⁸ The

¹⁸² See *Benedik v. Slovenia*. See also Council of Europe, *Conditions for Obtaining Subscriber Information in Relation to Dynamic versus Static IP Addresses: Overview of Relevant Court Decisions and Developments*, T-CY (2018)26, 25 October 2018.

¹⁸³ E-evidence Regulation, Art. 4.

¹⁸⁴ Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, [2008] OJ L 350, 30 December 2008, p. 7. See Art. 11(5) stating:

A Member State may, at the time of adoption of this Framework Decision, make a declaration or subsequent notification to the General Secretariat of the Council requiring such validation in all cases where the issuing authority is not a judge, a court, an investigating magistrate or a public prosecutor and where the measures necessary to execute the EEW would have to be ordered or supervised by a judge, a court, an investigating magistrate or a public prosecutor under the law of the executing State in a similar domestic case.

¹⁸⁵ E-evidence Regulation, Recital 61.

¹⁸⁶ Case C-399/11, *Melloni* [2013] ECLI:EU:C:2013:107, on the interpretation of Art. 53 of the Charter.

¹⁸⁷ Case C-105/14, *Taricco and Others* [2015] ECLI:EU:C:2015:555; Case C-42/17, *M.A.S. and M.B.* [2017] ECLI:EU:C:2017:936.

¹⁸⁸ When it comes to e-evidence, there is a profound interest to consider a situation as domestic. However, when it comes to bulk data interception by intelligence, the opposite is true. The states are interested to denominate the communication as ‘external’ to avoid national safeguards. See, e.g., the *Big Brother Watch* case, paras. 74–76. See also UK Parliament, Intelligence and Security Committee of Parliament, *Privacy and Security: A Modern and Transparent Legal Framework*, 12 March 2015, pp. 39–40, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

concept of extraterritorial application of the criminal code is not foreign to the criminal codes of EU member states¹⁸⁹ and EU criminal law.¹⁹⁰ The territoriality principle in criminal codes is often supplemented with the reality principle (e.g. on counterfeiting of money),¹⁹¹ the active personality principle (for acts committed by your citizen), the passive personality principle (for acts committed abroad against your citizen) or by the universality principle (e.g. for genocide, war crimes, crimes against humanity). The logic of such extension is to prevent impunity. However, extraterritorial application of criminal codes should be distinguished from jurisdiction.¹⁹² In principle, only national authorities have the power to exercise police and law enforcement powers in their territory. Any foreign intervention must be announced and confirmed. If not, it could be considered illegal and even criminal in nature. If law enforcement/judicial authorities were to conduct, for example, house searches or seizures on the territory of another state without permission, this would raise substantial legal and diplomatic issues as well as questions about the obligations of the different states involved as regards the protection of fundamental rights. The justification for a distinction between online and offline searches is not clear. States seem (too) relaxed when it comes to cross-border digital overreach. However, the ECHR is based on the territoriality principle.¹⁹³ Therefore, until now, cross-border measures in international mutual legal assistance (MLA)¹⁹⁴ instruments as well as under mutual recognition (such as controlled deliveries,¹⁹⁵ covert investigations,¹⁹⁶ joint investigation teams¹⁹⁷) were specifically

¹⁸⁹ For example, Strafgesetzbuch (German Criminal Code), BGBl. I. S. 3322, 13 November 1998, §§ 5–7, or Völkerstrafgesetzbuch (German International Criminal Code), BGBl. I. S. 2254, 26 June 2002, § 1; Code Pénal (French Criminal Code), JORF 169, 23 July 1992, Arts. 113–6 to 113–14; Ley Orgánica 6/1985, 1 July, del Poder Judicial (Spanish Law on the Judiciary); BOE-A-1985-12666, 1 July 1985, Art. 23; Kazenski zakonik (Slovenian Criminal Code), Ur. l. RS 55/08, 4 June 2008, Arts. 10 to 14; and so on.

¹⁹⁰ For example, Directive 2011/93/EU, Art. 17; Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, [2013] OJ L 218, 14 August 2013, Art. 12; Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law [2017] OJ L 198, 28 July 2017, Art. 11.

¹⁹¹ League of Nations, Geneva Convention for the Suppression of Counterfeiting Currency, Geneva, 20 April 1929, Arts. 8 and 9. See also Directive 2014/62/EU of the European Parliament and of the Council of 15 May 2014 on the protection of the euro and other currencies against counterfeiting by criminal law, and replacing Council Framework Decision 2000/383/JHA, [2014] OJ L 151, 21 May 2014, p. 1, Art. 8.

¹⁹² See B. J. George Jr, 'Extraterritorial Application of Penal Legislation' (1966) 64(4) *Michigan Law Review* 609–638.

¹⁹³ ECHR, Art. 1. This was extended to cases when state signatory has effective control due to military operations of the territory of another state. See *Loizidou v. Cyprus*, Appl. No. 15318/89, 18 December 1996, para. 52; *Cyprus v. Turkey*, Appl. No. 25781/94, 10 May 2001, para. 76; *Al-Skeini and Others v. United Kingdom*, Appl. No. 55721/07, paras. 130–150.

¹⁹⁴ See Council of Europe, Convention on Mutual Assistance in Criminal Matters (CoE MLA Convention), 20 April 1959 and its two additional protocols, and Council of Europe, Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (EU MLA Convention), 29 May 2000 and its additional protocol.

¹⁹⁵ Art. 12 of EU MLA Convention on controlled deliveries provides for permission of the requested state and respecting the procedures of that state. The same applies to Art. 18 of Second Additional Protocol to the CoE MLA Convention. Art. 28 of EIO Directive, based on mutual recognition, provides for an additional non-recognition ground ('would not be authorised in a similar domestic case'), whereby the executing authority has the right to act, to direct and to control operations.

¹⁹⁶ Art. 14 of EU MLA Convention on covert investigations provides for a decision on a case-by-case basis by the authorities of the requested state. Covert investigations must respect national law and the procedures of the state in the territory of which the investigation takes place. The same applies to Art. 19 of Second Additional Protocol to the CoE MLA Convention. Furthermore, according to Art. 29 of EIO Directive, two additional non-recognition grounds apply, namely the measure would not be authorised in a similar national case and no agreement could be reached.

¹⁹⁷ For a joint investigation team (JIT) a specific agreement is necessary; the team leader has to be from the member state where the team operates; the operations have to be carried out in accordance with the law of the state where the team operates; and seconded members can be entrusted with tasks agreed upon by both states. See EU MLA Convention, Art. 13; Second Additional Protocol to the CoE MLA Convention, Art. 20, and Council Framework Decision 2002/465/JHA on joint investigation teams, [2002] OJ L 162, 20 June 2002, p. 1.

regulated, including, inter alia, through an obligation to inform the state where the activity is taking place and to cease with the activity if not granted permission by the authorities of that state.

An exception is provided in Article 20 of the EU MLA Convention for the interception of communications without the help of another state. It applies when a legally ordered interception extends to the territory of another member state. In such a case, where the authority did not know beforehand that the subject is in the other territory, it must inform the notified state immediately when it becomes aware that the interception is on the territory of the latter state.¹⁹⁸ The notified state can confirm the measure within ninety-six hours. It can also prohibit the measure if it is not permissible under its law, is against public order or refers to a political offence, and it can require that the material obtained should not be used or should be used under certain conditions. It can also require a short extension, of up to a maximum period of eight days, to the original ninety-six-hour deadline, to be agreed with the intercepting member state, in order to carry out internal procedures under its national law. As long as the notified state has not made a decision, the measure can be applied. However, the material cannot be used, except if otherwise agreed between the member states concerned or for taking urgent measures to prevent an immediate and serious threat to public security.¹⁹⁹ A similar provision was included in Article 31 of the EIO Directive. However, the EIO Directive applies between judicial authorities only. In comparison, the EU MLA Convention provides also the possibility for non-judicial authorities to be considered as judicial ones for MLA purposes. It states that “competent authority” shall mean a judicial authority, or, where judicial authorities have no competence in the area covered by those provisions, an equivalent competent authority, specified pursuant to Article 24(1)(e) and acting for the purpose of a criminal investigation’.

The e-evidence approach is based on direct orders by the issuing state, without the involvement of the enforcing state. The same logic was used in the US *Microsoft* case²⁰⁰ and followed by the US CLOUD Act.²⁰¹ In the *Microsoft* case, the provider opposed a US search warrant that directed it to produce the contents of one of its customers’ emails where that information was stored on a server located in Ireland. However, such a logic raises the issue of conflict with third-country law.²⁰² At the 2018 European Parliament hearing on the e-evidence, ECHR Judge Bošnjak stated:

High Contracting Parties to the ECHR, including all 28 MS EU, are responsible for protection of human rights on the territory under their jurisdiction. . . . If the authorities of the enforcing state are faced with a complaint that the protection of a Convention right has been manifestly deficient and this cannot be remedied by EU law, they cannot refrain from examining the complaint on the ground that they are just applying EU law. . . . The proposal, as it is before you, creates a rather unique situation from the point of ECHR jurisprudence. The interferences with Article 8 are without any involvement of the authorities of the enforcing state. I wonder if this is in line with the ECHR.²⁰³

¹⁹⁸ EU MLA Convention, Art. 20(2)(b).

¹⁹⁹ EU MLA Convention, Art. 20(4). According to Art. 20(7), a state can declare that it will not be necessary to provide it with information on interceptions. However, it seems that none of the member states used this option.

²⁰⁰ *In re Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp. v. United States*, 15 F. Supp. 3d 466 (SDNY 2014), deciding against the plaintiff; *In re Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp. v. United States*, 829 F. 3d 197 (2d Cir. 2016), deciding for the plaintiff; and *United States v. Microsoft Corp.*, 138 S. Ct 1186 (2018), no decision taken due to the adoption of the US CLOUD Act. See also M. Rutherford, ‘The Cloud Act: Creating Executive Branch Monopoly over Cross Border Data Access’ (2020) 34(4) *Berkeley Technology Law Journal* 1177–1204; J. Daskal, ‘Privacy and Security Across Borders’ (2019) *Yale Law Journal Forum* 1029–1051, www.yalelawjournal.org/pdf/Daskal_np47txze.pdf.

²⁰¹ Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of 2018, www.justice.gov/criminal/cloud-act-resources.

²⁰² E-evidence Regulation, Art. 16 providing for a specific conflict of law dispute procedure.

²⁰³ See LIBE Committee, 2nd Working Document on the Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (2018/0108 (COD)) – Scope of application and

It is also clear from ECtHR case law on civil and criminal mutual recognition cases,²⁰⁴ in connection with the *Bosphorus*²⁰⁵ presumption of equivalent protection of fundamental rights in the EU, that the affected executing/enforcing state must have the opportunity to react. Also a state that is only helping another in cross-border MLA (or another form) can be found to violate fundamental rights. However, during legislative negotiations, the European Parliament moved from a notification approach with suspensive effect for all traffic and content data to a more limited notification for such data only in ‘non-domestic cases’.²⁰⁶ As explained earlier, the lack of clarity about the terms ‘domestic’ and ‘residence’ allows for possible misuse. Consequently, a notification with suspensive effect providing for the enforcing state the option to be fully informed and to stop the transfer will be very limited in practice under the EU e-evidence system. Questions on and challenges to the compatibility of the whole system with the ECHR and the national constitutions are to be expected.

1.5 CONCLUSIONS

Based on an analysis of the EU digital and security strategies, the broader digital framework and some recent legislative proposals relating to it, certain conclusions can be drawn. Firstly, recent developments indicate a shift from the suspect and his or her individual rights to a more preventive perspective, namely, a focus on effective tools for law enforcement. There is a blurring of the lines between the private sector and law enforcement, as well as backtracking from the classical safeguards established in EU cross-border cooperation in the last twenty years. Some of the instruments (e-evidence) allow for the authorisation of orders by prosecutorial authorities only and exclude the possibility of checks in the enforcing state. Others allow intrusions into privacy without a prior suspicion by private providers only (on protection of children). Secondly, a cacophony of strategies, sub-strategies and agendas makes it difficult to understand their interplay. They sometimes deliver contradictory messages, for example a call for an open society coupled with zero tolerance for crime.²⁰⁷ Thirdly, there is a possible lack of an established EU philosophy on democracy, fundamental rights and data privacy in the digital age. Actions sometimes seem driven by more momentary considerations, for example on the fight against terrorism. However, a coherent coordination between them is sometimes missing (e.g. DSA and TCO). Fourthly, the Security Agenda shows a certain tendency to establish a surveillance society. Fifthly, most of the mentioned EU instruments use Article 114 TFEU on the internal market as their legal basis, and not justice and home affairs, data protection or crime prevention (Articles 16, 82 or 87 TFEU). This indicates an underestimation of the far-reaching consequences of such instruments for the right to privacy and other rights. It is true that what is illegal offline should also be illegal online. However, the same should apply to privacy, data protection and procedural safeguards. Law enforcement authorities and others should not conduct online investigations that would be illegal if they were conducted in the physical

relation with other instruments, [2019] DT\1176230EN, 6 February 2019; European Parliament, 3rd Working Document on the Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (2018/0108 (COD)) – Execution of EPOC(-PR)s and the role of service providers, [2019] DT\1176298EN, 6 February 2019.

²⁰⁴ *Avotiņš v. Latvia*, Appl. No. 17502/07, 23 May 2016, paras. 101 and 112; *Pirozzi v. Belgium*, Appl. No. 21055/11, 17 April 2018, paras. 63–64; *Romeo Castaño v. Belgium*, Appl. No. 8351/17, 9 July 2019, para. 84.

²⁰⁵ *Bosphorus v. Ireland*, Appl. No. 45036/98, 30 June 2005, paras. 155–156.

²⁰⁶ See Section 1.3.1 of this chapter.

²⁰⁷ You cannot have zero crime and an open society. A zero-crime policy online entails as a practical consequence a permanent monitoring/surveillance of online activity. Hence, it does not lead to a free society.

world. Consequently, there is a certain danger that the EU will not take the lead as a worldwide standard setter in the protection of privacy and data protection in the digital age by achieving a reasonable balance between such rights and effective law enforcement; rather, it might trail and mimic preventive state models that use technology for full-scale preventive surveillance with minimal or no privacy, lack of prior suspicion, absence of both court oversight and effective remedies, as well as blurring the lines between intelligence and law enforcement, and state agents and private companies, while paying ‘lip service’ to fundamental rights. This should not be the case. We can see such developments in view of the negative potential of modern technology in other parts of the world.

Unresolved Jurisdictional Issues in Law Enforcement Access to Data

Dan Svantesson and Anna-Maria Osula^{*}

2.1 INTRODUCTION

Effective law enforcement carried out in accordance with fundamental rights is a state obligation. This state obligation applies whether or not the offender is in the same state as the victim. Thus, in some cases, states have a responsibility to investigate crimes committed by foreign offenders. This places considerable stress on law enforcement agencies (LEAs). It may also place stress on international relations, and it poses significant challenges for the proper protection of fundamental rights.

To be effective, LEAs need adequate access to evidence. Such access is essential both for the conviction of criminals and for the protection of those wrongly accused. The increasingly sophisticated realm of crime now more than ever involves challenges related to the access of digital evidence, and employing such evidence in court, because most offences involve actors, actions or substantial effects that are wholly or in some part located or have been carried out in different jurisdictions. Therefore, relevant evidence may not always be located in domestic territory. In such cases, getting time-critical access to evidence may require the assistance of both industry and law enforcement partners from around the world.

To make things even more complicated, due to the decentralised nature of cyberspace, the targeted evidence may be residing in multiple jurisdictions at once or it may be impossible to identify the location at all at a given time (a phenomenon also known as ‘loss of knowledge of location’ or more commonly, but less accurately, ‘loss of location’, discussed further in Section 2.2.4). This may easily occur in cloud computing where, in order to provide the user with seamless interaction between multiple applications and services, different applications and servers across various locations are used at the same time. Consequently, the identification

^{*} The authors’ contribution to this chapter is based on research supported by Masaryk University project no. CZ.02.1.01/0.0/0.0/16_019/0000822 (C4E). Any views or opinions expressed in this chapter are personal and do not represent those of institutions or organisations that the authors are associated with in their professional capacity. This chapter draws, and expands, upon research findings discussed in a range of the authors’ previous works in the field, in particular: D. Svantesson *Solving the Internet Jurisdiction Puzzle* (Oxford: Oxford University Press, 2017); R. Polcak and D. Svantesson *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law* (Cheltenham: Edward Elgar, 2017); D. Svantesson, ‘European Union Claims of Jurisdiction over the Internet – An Analysis of Three Recent Key Developments’ (2018) 9 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 113–125; D. Svantesson and L. van Zwieten, ‘Law Enforcement Access to Evidence via Direct Contact with Cloud Providers – Identifying the Contours of a Solution’ (2016) 32 *Computer Law & Security Review* 671–682; D. Svantesson, ‘Preliminary Report: Law Enforcement Cross-Border Access to Data’, 22 November 2016, <http://dx.doi.org/10.2139/ssrn.2874238>; A.-M. Osula, ‘Transborder Access and Territorial Sovereignty’ (2015) 31(6) *Computer Law & Security Review* 719–735; A.-M. Osula, ‘Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study’ (2016) 24(4) *International Journal of Law and Information Technology* 343–373; A.-M. Osula, ‘Remote Search and Seizure of Extraterritorial Data’, PhD thesis, University of Tartu, 2017.

of the location of certain data in cloud computing is more complex as data could be spread across these applications and servers. Additionally, digital evidence stored in the cloud is not exclusively relevant for the domain of cybercrime.

It is estimated that more than five billion users have access to the internet,¹ and, not least due to the widespread use of connected devices (so-called Internet of Things), more and more data is being produced and processed, such that the total amount is expected to reach 175 zettabytes in 2025.² This new digital reality brings attention to the fact that current and future criminal investigations must take into account the unique characteristics of the internet as well as evidence either stored on or transmitted via electronic devices. The jurisdictional challenges are severe but must be overcome.

In this chapter we first discuss a selection of particularly potent normative challenges. We then examine a range of traditional and novel tools aimed at ensuring LEAs' cross-border access to evidence, before reaching some conclusions on the jurisdictional challenges.

2.2 NORMATIVE CHALLENGES

As noted, cross-border access to digital evidence is necessary for effective international cooperation in criminal investigations and the fight against crime. However, the development of regulation of such investigative measures should keep in mind several challenges and must be constructed taking into account the complex matrix of important rights and interests at stake.³ For example, several countries are making efforts in strengthening domestic data protection law. The cloud providers, or other entities, that may be subject to law enforcement requests for data have a duty to be respectful of the human rights of their customers (such as data privacy), as well as non-customers whose data they end up holding due to the activity of their customers.⁴ This duty flows from a range of human rights treaties, such as the International Covenant on Civil and Political Rights, and in the context of Europe the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union 2000, which contains a specific right to the protection of personal data.

However, it seems that cloud providers currently hold different views on how fundamental rights guide their actions in relation to LEA requests. While rights such as the right to privacy and protection of personal data are fundamental, they are not absolute – in other words, they are constantly subject to reconciling and/or balancing exercises involving other, sometimes (in a given context) competing, fundamental human rights.

Additionally, the legal assessment of (unilateral) cross-border access to data not stored domestically should be analysed together with concepts of international law such as jurisdiction to enforce,⁵ territorial sovereignty and reciprocity. Reciprocity may play an important role in situations where State A (which has strong data protection safeguards) accesses data on the

¹ Statistics 2022, ITU, www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

² European Commission, 'A European Strategy for Data' (COM(2020) 66 Final), 19 February 2020, 2.

³ See further Svantesson and Zwieten, 'Law Enforcement Access', 671–682.

⁴ The relation between data protection and criminal investigations/law enforcement is analysed in more detail in Chapter 3 in this volume.

⁵ Commonly, the jurisdiction to take executive or judicial action in pursuance of laws and decisions is known as jurisdiction to enforce and is normally seen to include law enforcement activities such as investigation. According to the Lotus Principle, no state may exercise its power in any form in the territory of another state unless based on a permissive rule derived from international custom or from a convention. The Case of the *SS Lotus*, *Fr v. Turk*, 1927 PCIJ (ser. A) No. 10 (Decision No. 9) (Permanent Court of International Justice), para. 45.

territory of State B (with weak data protection safeguards). In such a case, it may not be desirable for State A that State B would in similar manner access data stored on its territory.

Here, we examine six normative challenges in more detail. In particular, we focus on:

- (1) the fact that criminal investigations give rise to a variety of jurisdictional claims;
- (2) the current move away from a strict focus on territoriality;
- (3) the uncertain role of sovereignty;
- (4) issues associated with so-called loss of location;
- (5) the distinction between single-factor test versus multi-factor tests; and
- (6) situations where regulatory compliance may be impossible.

2.2.1 Jurisdiction Over What?

The first matter of jurisdiction that arises in a criminal investigation is whether the investigator (be it the police, a prosecutor or an investigative judge) has jurisdiction over the offence to be investigated. On a theoretical level, the answer to that matter will depend on both domestic jurisdictional law and international law. But, in practice, investigators will, often legitimately, assume that the domestic jurisdictional law they work with is in line with international law. Thus, on a practical level, domestic jurisdictional law is determinative.

Where it is concluded that the investigator has jurisdiction over the offence to be investigated, another type of jurisdictional issue arises – an issue of key concern – that is, does the investigator have jurisdiction to take the investigative measures it wishes to pursue? Traditionally, this has been viewed as a matter of ‘enforcement jurisdiction’, and has thus been grouped together with, and subjected to the same restrictions placed on, completely different types of action.

This distinction between jurisdiction over the offence and jurisdiction over the evidence is clearly articulated in the Budapest Convention. Article 22, the provision that deals in general terms with the topic of jurisdiction, relates only to jurisdiction over the offences prescribed in the Budapest Convention (i.e., Articles 2 through 11), and does not govern jurisdiction over the evidence.

In more detail, when public international law speaks of jurisdiction, it typically divides jurisdiction into three different categories:

- (1) prescriptive (or legislative) jurisdiction;
- (2) judicial (or adjudicative) jurisdiction; and
- (3) enforcement jurisdiction.

Prescriptive (or legislative) jurisdiction relates to the power to make law in relation to a specific subject matter. Judicial (or adjudicative) jurisdiction, as the name suggests, deals with the power to adjudicate a particular matter. Finally, enforcement jurisdiction relates to the power to enforce the law put in place, in the sense of arresting, prosecuting and punishing an individual under that law.

When we debate law enforcement access to data, we typically seem to discuss it as an exercise of enforcement jurisdiction. Enforcement jurisdiction is closely tied to the territoriality principle because we generally do not want, for example, law enforcement agents from one country kidnapping suspects in other countries like in the famous *Eichmann* case.

But law enforcement access to data is, of course, very different from cross-border kidnapping, and the fact that public international law groups the two together reveals an inexcusable lack of sophistication. It quite simply does not make sense to bundle matters such as the investigation

into what data is stored on a foreign server with matters such as the *Eichmann* case. They have little in common, and we need to accept a lower jurisdictional threshold in relation to the former situation than we do in relation to the latter situation. More recently, there is a clear trend of investigative measures being treated as something markedly different, and ‘investigative jurisdiction’ as a separate category of jurisdiction – distinct from enforcement jurisdiction – is gaining recognition.

2.2.2 *Jurisdiction to Enforce and a Move Away from Territoriality*

While jurisdiction is linked to the concept of territory, it is not exclusively tied to it,⁶ which means that the principle of territoriality cannot always be applied in a straightforward manner.⁷ For instance, a state could employ prescriptive or adjudicative jurisdiction over an extraterritorial matter by, for example, using the nationality principle in order to extend its material jurisdiction to its citizens located in another country. Or a state could argue that based on the ubiquity theory the subjective territoriality principle (referring to the location of the criminal conduct) or the objective territoriality principle (referring to the result of the criminal conduct) is applicable when part of the offence has taken place in a foreign territory. Furthermore, some states support the, some would say controversial, ‘effects doctrine’ – the extraterritorial application of which would require a ‘genuine connection between the subject matter of jurisdiction and the territorial base or reasonable interests of the state in question’.⁸ Apart from the general challenges that fighting cybercrime poses to applying traditional notions of law, problems related to prescribing prescriptive or adjudicative jurisdiction have not been reported extensively.⁹

Nevertheless, there is an apparent difference between the legally accepted territorial scope of different functions of jurisdiction. Even if it is accepted that a state could apply prescriptive or adjudicative jurisdiction over an extraterritorial matter, under a traditional public international law view, states generally lack the jurisdiction to enforce their decision on the territory of the other state.¹⁰ Thus, it would, for example, be illegal for a state to send police forces to another state’s territory or to exercise an act of administration or jurisdiction on foreign territory without permission,¹¹ resulting in violating both international law and the domestic legal framework (e.g., provisions of the domestic Penal Code),¹² and also possibly hindering peaceful relations between states.¹³

⁶ Malcolm N. Shaw, *International Law* (Cambridge: Cambridge University Press, 2008), 646.

⁷ R. Jennings and A. Watts (eds.), *Oppenheim’s International Law*, 9th ed. (London: Longman, 1996), vol. I, 458.

⁸ J. Crawford, *Brownlie’s Principles of Public International Law*, 8th ed. (Oxford: Oxford University Press, 2012), 457.

⁹ United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime: Draft – February 2013* (Vienna: UNODC, 2013), xvii, xxv, www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG_4_2013/CYBERCRIME_STUDY_210213.pdf. See, e.g., Svantesson, *Solving the Internet Jurisdiction Puzzle*, 159–167. See also Susan W. Brenner and Bert-Jaap Koops, ‘Approaches to Cybercrime Jurisdiction’ (2004) 4(1) *Journal of High Technology Law*, <https://ssrn.com/abstract=786507>.

¹⁰ International Court of Justice, *Democratic Republic of Congo v. Belgium, Arrest Warrant of 11 April 2000*, 14 February 2002, 168, www.icj-cij.org/case/121.

¹¹ Crawford, ‘Brownlie’s Principles’, 386–387.

¹² E.g., Article 271, para. 1 of the Swiss Criminal Code (of 21 December 1937, status as of 26 July 2021) prescribes:

Any person who carries out activities on behalf of a foreign state on Swiss territory without lawful authority, where such activities are the responsibility of a public authority or public official, any person who carries out such activities for a foreign party or organisation, any person who encourages such activities, is liable to a custodial sentence not exceeding three years or to a monetary penalty, or in serious cases to a custodial sentence of not less than one year.

¹³ Mireille Hildebrandt, ‘Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace’ (2013) 63(2) *University of Toronto Law Journal* 196, 223.

However, as noted already, it is questionable whether the type of investigative measures focused on in our discussion should be viewed as a form of ‘enforcement jurisdiction’. Further, the rules for the territorial scope of jurisdiction to enforce are not explicit in cyberspace. Unlike in the ‘physical world’ where exercising jurisdiction to enforce would generally mean physically being on another state’s territory without prior authorisation and where the transgressing agents may be caught and convicted according to the domestic law of the captor state,¹⁴ investigative measures such as remote search and seizure of extraterritorial data do not require the state agents to leave their domestic territory, rendering such national remedies largely unavailable.¹⁵ Indeed, if the officers conducting the investigation do not leave their own territory, would there be any ground for discussing extraterritorial application of jurisdiction to enforce, and thereby a possible breach of sovereignty? This was also central in the matter between Microsoft and the US government, discussed in Section 2.3.3.¹⁶

Since much of the law regarding jurisdiction has developed through the decisions of national courts applying domestic laws, sometimes irrespective of their compatibility with international law, the influence of national jurisprudence has contributed to the uncertainty surrounding many matters related to jurisdiction.¹⁷ Based on scarce evidence of state practice, available (and often contradictory) case law and limited discussion (at least in English language literature) on the ‘location’ of investigative measures such as remote access, three broad approaches can be distinguished.

It has been discussed in literature that in situations where law enforcement finds a networked computer that is displaying data, normally stored abroad, on the screen, and that has also stored the data in the interim memory of the computer, such a copy would be, strictly speaking, located in the domestic jurisdiction,¹⁸ and hence, accessing such data would not entail an application of extraterritorial jurisdiction to enforce. Building on this reasoning, holders of this first view believe that an extraterritorial search is legal in circumstances where the agents, while surreptitiously installing data extraction software,¹⁹ or employing other investigative measures with an extraterritorial reach, do not actually leave the judicial district to obtain and view the information gathered from the target computer, since the data will first be examined within their domestic territory and becomes ‘property located within the district’.²⁰ According to this logic, law enforcement could ‘roam the world’ in search of a ‘container of contraband’ so long as the data container is not opened until the ‘agents haul it off to the issuing district’,²¹ or, in other words, until the agents actually view the data strictly on the territory where the warrant for accessing the data was granted.

This is also consistent with the view that ‘a search occurs when information from or about the data is exposed to possible human observation, such as it appears on a screen, rather than when it is

¹⁴ Antonio Cassese, *International Law*, 2nd ed. (Oxford: Oxford University Press, 2005), 51.

¹⁵ Note that there have been cases where individuals have been charged for illegal access or similar offences without being physically present on the territory of that state. See, e.g., United States Department of Justice, Office of Public Affairs, ‘U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage’, 19 May 2014, www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor; *United States v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui*, 14–118 (2014).

¹⁶ *United States v. Microsoft Corp.*, 138 S. Ct 1186 (2018).

¹⁷ Crawford, ‘Brownlie’s Principles’, 457.

¹⁸ Nicolai Seitz, ‘Transborder Search: A New Perspective in Law Enforcement?’ (2004) 7 *Yale Journal of Law & Technology* 23, 28.

¹⁹ ‘In the Matter of a Warrant to Search a Target Computer at Premises Unknown’ [2013], 958 F. Supp. 2d 753, 758.

²⁰ *Ibid.*, 4.

²¹ *Ibid.*, 5.

copied by the hard drive or processed by the computer’,²² allowing, for example, the US District Court to conclude that since no exposure to the domestic law enforcement takes place until the data is being reviewed in the US (i.e., the state accessing the information), ‘no extraterritorial search has occurred’.²³ The second perspective suggests that such a search actually takes place in two locations: one, where the computer that is the target of the search resides, and another, where the data will actually be analysed by the other state’s law enforcement.²⁴

The third view, however, asserts that the collection of extraterritorially located data via investigative techniques such as remote search and seizure would indeed take place in foreign networks. This perspective was supported by a US District Court decision stating that ‘[s]uch search takes place, not in the airy nothing of cyberspace, but in physical space with a local habitation and a name’, and, even when the search could be seen as twofold, ‘[n]either search will take place within this district’.²⁵ The same approach has been echoed by Microsoft in the earlier mentioned *Microsoft Warrant* case, which maintained that ‘[a] seizure of electronic mail occurs at the time it is copied and in the place where it is stored’²⁶ and by a US Second Circuit judgment asserting that ‘the invasion of the customer’s privacy takes place ... where the customer’s protected content is accessed – here, where it is seized’.²⁷

Also, several court rulings in the so-called *Playpen* case which have focused on the legality of a certain investigative technique also concur that the property to be searched is the final destination (i.e., the user’s computer rather than the server where the investigative measures have been launched from).²⁸ Similarly, a number of scholars have concluded that during a cross-border search, the government action takes place outside the state which is conducting the search since what matters is the ‘end result of the search’²⁹ and that a ‘search of one’s hard drive by a foreign [law enforcement] agency from abroad ... has the same effects as a traditional search of premises’, therefore, ‘the consent of the territorial sovereign in which the target is located is required’.³⁰ It can thus be concluded that even if we differentiated between ‘search’ and ‘seizure’ activities, the latter would still entail the act of ‘copying the data’, necessarily taking place in extraterritorial networks, and consequently understood as an extraterritorial application of jurisdiction to enforce. This approach was also recognised by the US Department of Justice, which cautioned that ‘some countries may object to attempts by US law enforcement to access computers located within their borders. Although the search may seem domestic to a US law enforcement officer executing the search in the US pursuant to a valid warrant, other countries may view matters differently.’³¹

²² Orin S. Kerr, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 3rd ed. (Washington, DC: Office of Legal Education Executive Office for United States Attorneys, 2009), 23.

²³ *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.* [2014], 15 F. Supp. 3d 466, 13–14.

²⁴ Orin Kerr, ‘Fascinating New Case on Legal Standards for Searching a Remote Computer with Unknown Location’, Volokh Conspiracy, 26 April 2013, <http://volokh.com/2013/04/26/fascinating-new-case-on-legal-standards-for-searching-a-remote-computer-with-unknown-location/>.

²⁵ ‘In the Matter of a Warrant to Search a Target Computer at Premises Unknown’, 5–6.

²⁶ Brief in support of appellant, *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, [2014] 14-2985-cv (2nd Cir. 2014), 31.

²⁷ *Microsoft v. United States*, No. 14-2985 (2nd Cir. 2016), 39.

²⁸ E.g., *United States v. Levin*, 15-10271-WGY, 2016 WL 2596010 (D. Mass. 2016), 14; *United States v. Arterbury*, 15-CR-182-JHP, 2016 BL 133752 (N.D. Okla. 2016), 16.

²⁹ Stewart M. Young, ‘Verdugo in Cyberspace: Boundaries of Fourth Amendment Rights for Foreign Nationals in Cybercrime Cases’ (2003) 10(1) *Michigan Telecommunications & Technology Law Review* 139.

³⁰ Stephan Wilske and Teresa Schiller, ‘International Jurisdiction in Cyberspace: Which States May Regulate the Internet?’ (1997) 50(1) *Federal Communications Law Journal* 117, 174.

³¹ *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 85.

However, at the same time, it is clear from emerging state practice that investigational needs and the increasing sophistication of cybercrime are pushing countries towards slowly but steadily altering the level of acceptance for the limits of jurisdiction to enforce, ultimately rendering the traditional understanding less relevant. This is also evident from the ongoing EU reforms where in public documents issued by the EU there has been very limited discussion on the scope and limits of jurisdiction to enforce.

An alternative to the problematic territoriality focus can be found in a framework outlining what is argued to be three jurisprudential core principles for jurisdiction more broadly. Adopted to the present context, they would dictate that where an investigator seeks cross-border access to electronic evidence, (s)he needs to show that:

- (1) there is a substantial connection between the matter in relation to which the investigative measure is taken and the state seeking to exercise investigative jurisdiction;
- (2) the state seeking to exercise investigative jurisdiction has a legitimate interest in the investigative measures in question; and
- (3) the exercise of investigative jurisdiction is reasonable given the balance between the state's legitimate interests in the investigative measures in question and other interests.³²

Much work obviously lies ahead in defining, as precisely as possible, what is meant by 'legitimate interest' and 'substantial connection', and the challenge of reaching consensus on the balancing of interests as part of the third principle should not be underestimated. Nevertheless, multi-stakeholder work to define these concepts is already underway³³ and there are precedents to draw upon, such as the system under which one country can proceed, for example in regard to wiretapping, without seeking prior consent from another country. If we can agree that it is the challenges associated with fleshing out the framework for investigative jurisdiction, canvassed earlier, that we should focus on, we have already made tremendous progress towards a framework for tackling the issue of cross-border access to electronic evidence.

2.2.3 Breaching Sovereignty

Regardless of views that cross-border access would generally be in line with territorial sovereignty,³⁴ neither individual countries nor international organisations have univocally supported such access without any additional legal grounds such as consent; nor does the legality of cross-border access appear widely defended by scholars.³⁵ Furthermore, there are well-known instances, such as the *Gorshkov-Ivanov*³⁶ and *Bredolab* botnet

³² See, e.g., D. Svantesson, 'A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft' 109 (2015) *American Journal of International Law Unbound* 69; Svantesson, *Solving the Internet Jurisdiction Puzzle*; Polcak and Svantesson, *Information Sovereignty*.

³³ Internet & Jurisdiction Policy Network, 'Data & Jurisdiction Program', www.internetjurisdiction.net/work/data-jurisdiction.

³⁴ E.g., Jack L. Goldsmith, 'The Internet and the Legitimacy of Remote Cross-Border Searches' (2001) 16 *Public Law and Legal Theory Working Papers* 115.

³⁵ E.g., B.-J. Koops and M. Goodwin *Cyberspace, the Cloud, and Cross-Border Criminal Investigation* (Tilburg: Tilburg University Press, 2014), 9 on the strict interpretation of international law according to which transborder access without the consent of the foreign state constitutes a wrongful act under international law; Patricia L. Bellia, 'Chasing Bits Across Borders' (2001) *University of Chicago Legal Forum* 100 generally concluding that unilateral transborder access would be prohibited by customary international law; Council of Europe, Explanatory Report to the Convention on Cybercrime, ETS No. 185, 23 November 2001, para. 161, reaching the conclusion that customary law regarding transborder access does not exist at all.

³⁶ *United States v. Gorshkov*, 2001 WL 1024026 (2001).

cases,³⁷ where the employment of effective investigation techniques may be seen as challenging the traditional understanding of territorial sovereignty. Overall, in assessing whether accessing data that is located in a foreign jurisdiction without sufficient grounds in international law would be a breach of sovereignty, two substantially different viewpoints have emerged.

The first is based on the strict interpretation of the ‘vehemently criticised’³⁸ *Lotus* case, according to which any exercise of jurisdiction to enforce on a foreign territory should be considered a violation of territorial sovereignty. According to this approach, unless on specific legal grounds, the territorial limitations of conventional investigative powers, such as search and seizure, do not allow for cross-border access to servers located in other jurisdictions.³⁹ Should such access occur, it would constitute a breach of sovereignty even if the mere ‘virtual presence’ would not cause any damage to the transgressed state’s networks.⁴⁰ The Netherlands has also underlined that traditionally the act of exercising investigative powers in a cross-border context would be deemed a violation of a country’s sovereignty unless the country in question has explicitly granted permission (by means of a treaty or other instrument).⁴¹ However, as a consequence of such a low legal threshold, there could possibly be thousands of breaches of sovereignty every day, and this could become very burdensome for states. Possibly, countries’ decisions not to respond to such ‘breaches’ of sovereignty may be strategic so as to allow a wide range of possible interpretations and ‘room for action’; the legal uncertainty of the legal status under international law is similar to the often-quoted example of cyber espionage.⁴²

³⁷ BBC, ‘Dutch Police Use Unusual Tactics in Botnet Battle’, 27 October 2010, www.bbc.com/news/technology-11635317. Whereas it is unlikely that someone would bring the Dutch police to justice for the advisory messages they sent to computers worldwide, the action does draw attention to the legal limits of law enforcement’s activities in regard to computers located in foreign territories.

³⁸ Cedric Ryngaert, *Jurisdiction in International Law*, 2nd ed. (Oxford: Oxford University Press, 2015), 34. See also Paul de Hert, ‘Cybercrime and Jurisdiction in Belgium and the Netherlands: Lotus in Cyberspace – Whose Sovereignty Is at Stake?’, in Bert-Jaap Koops and Susan W. Brenner (eds.), *Cybercrime and Jurisdiction: A Global Survey* (Den Haag: TMC Asser, 2006), 72; Svantesson, *Solving the Internet Jurisdiction Puzzle*, 15–24.

³⁹ E.g., Steven Chong SC, ‘Keynote Address by the Honourable Attorney-General’, Criminal Law Conference, 17 January 2014, 10, [www.agc.gov.sg/docs/default-source/speeches/2014/ag-speech_criminal-law-conference_17-jan-2014-\(1\).pdf](http://www.agc.gov.sg/docs/default-source/speeches/2014/ag-speech_criminal-law-conference_17-jan-2014-(1).pdf).

⁴⁰ Wolff Heintschel von Heinegg, ‘Territorial Sovereignty and Neutrality in Cyberspace’ (2013) 89 *International Law Studies* 123, 129; Koops and Goodwin, *Cyberspace, the Cloud*, 9, 61–62. However, the Tallinn Manual experts were unable to concur whether a country’s activity that does not cause any damage to another state, such as planting malware for monitoring, could be considered a breach of sovereignty. Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 16. This conclusion should be separated from their legal assessment of conducting inherently governmental functions exclusively reserved to another state on the latter’s territory, see Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge: Cambridge University Press, 2017), 22–23.

⁴¹ United Nations General Assembly, *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266* (2021), 56–57.

⁴² Robert D. Williams, ‘(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action’ (2011) 79(4) *George Washington Law Review* 1175. It should be noted that there is general legal ambiguity regarding the legality of cross-border collection of data. Over the years, nations have collected information from the territory of another nation with the help of, e.g., binoculars, periscopes and orbital reconnaissance satellites without physically entering the territory and these activities, often labelled espionage, appear not to be prohibited under international law. See, e.g., Goldsmith, ‘The Internet and the Legitimacy of Remote Cross-Border Searches’, p. 114. However, it is unclear whether the legal assessment for state activities aimed at collecting intelligence in the form of espionage can be equalled with state carrying out remote search and seizure procedures for collecting extraterritorial evidence for criminal proceedings. See also Schmitt, *Tallinn Manual 2.0*, where it was concluded that a state may not conduct

The second, alternative view emphasises that not every state conduct that has an impact on the cyber infrastructure of another state would necessarily constitute a violation of the principle of territorial sovereignty.⁴³ There are different ways of understanding this claim. In order to be seen as a violation of the territoriality principle, the extraterritorial access should result in inflicting material damage to the cyber infrastructure located in the other state; an act resulting in mere minor material damage to the cyber infrastructure should not be considered a violation of territorial sovereignty.⁴⁴ Supporters of this view maintain the general legitimacy of searches which do not inflict material damage and argue that ‘remote crossborder searches fit into the long-accepted practice of officials in one nation acting within their territory (or from public spaces) to extract information from another’ and that ‘territorial sovereignty has never had a definitive content’.⁴⁵

Further support for this thinking may be found by comparing the topic of law enforcement cross-border access to data to other fields. Consider, for example, a situation where a court in State A orders a company in State B to delete data that the company holds on a server in State B. This happens frequently, for example, in the fields of intellectual property, defamation and hate speech. In such situations, no one seems concerned about the implications for State B’s territorial sovereignty. Yet in this type of situation the exercise of jurisdiction by State A is more severe in that data is actually deleted in State B rather than merely accessed, as is the case in the scenarios discussed here of law enforcement seeking access to data in a foreign state where the foreign state may (1) lack awareness of the data, (2) be unable to access the data or (3) lack any discernible interest in the data. Counterarguments to this viewpoint are that if cross-border searches are to be declared legal under international law, they may be abused by states and such searches could foment reciprocity.⁴⁶

The alternative approach to the requirement to result in inflicting damage is focusing on a specific object or governmental function. Accordingly, it can be argued that any interference with an object enjoying ‘sovereign immunity’ such as diplomatic premises should be seen as a violation of the sovereignty of that state.⁴⁷ Similarly, the experts of the Tallinn Manual 2.0 concluded that a state may not conduct inherently governmental functions exclusively reserved to another state on the latter’s territory; therefore, for example, if a state were to conduct a law enforcement operation against a botnet in order to obtain evidence for criminal prosecution by taking over its command and control servers located in the other state without that state’s consent, the former would violate the latter’s sovereignty because the operation would usurp an inherently governmental function exclusively reserved to the territorial state under international law.⁴⁸

As this discussion shows, international law remains unsatisfactorily unclear about whether cross-border investigative techniques such as remote search and seizure constitute a violation of

inherently governmental functions exclusively reserved to another state on the latter’s territory; and therefore, for example, if a state were to conduct a law enforcement operation against a botnet in order to obtain evidence for criminal prosecution by taking over its command and control servers located in the other state without that state’s consent, the former would violate the latter’s sovereignty because the operation usurps an inherently governmental function exclusively reserved to the territorial state under international law. Williams, ‘(Spy) Game Change’; Schmitt, *Tallinn Manual 2.0*, 22–23.

⁴³ Wolff Heintschel von Heinegg, ‘Legal Implications of Territorial Sovereignty in Cyberspace’, 2012 4th International Conference on Cyber Conflict, 5–8 June 2012, 11.

⁴⁴ *Ibid.*

⁴⁵ Koops and Goodwin, *Cyberspace, the Cloud*, 108.

⁴⁶ *Ibid.*, 116.

⁴⁷ Heintschel von Heinegg, ‘Territorial Sovereignty’, 130.

⁴⁸ Schmitt, *Tallinn Manual 2.0*, 22–23.

sovereignty. The Netherlands has pointed out that from the perspective of law enforcement, the manner in which the principle of sovereignty should be applied has not fully crystallised at international level and that opinion is divided as to what qualifies as exercising investigative powers in a cross-border context and when it is permissible without a legal basis founded in a treaty.⁴⁹ In the opinion of the authors, the unclear status of cross-border investigative techniques without further legal grounds or consent cannot be considered today as a ‘constant and uniform practice of states . . . in circumstances which give rise to a legitimate expectation of similar conduct in the future’,⁵⁰ such that it could be seen as a rule of international customary law.

However, a conclusion that such conduct does indeed amount to a breach of territorial sovereignty of the other state may be seen to be supported by the increasingly rich evidence of international organisations and states making an effort to identify legitimate grounds for cross-border investigative techniques such as remote search and seizure, be it by means of treaty provisions or within domestic frameworks. Several countries are looking for or have identified grounds for precluding, in a transparent manner, the potential wrongfulness of such searches under international law in order to make sure the activities would not be regarded as a breach of other states’ sovereignty. In parallel, interviews with practitioners confirmed that if the location of the data to be searched is known to be on the territory of a specific state, mutual legal assistance (MLA) procedures or other state-to-state mechanisms should be preferred.⁵¹

2.2.4 ‘Loss of Location’

Among the circumstances that have been proposed to be excluding the wrongfulness of remote search and seizure of extraterritorial data, loss of location may be seen as the most prevalent justification for cross-border access used by states in justifying their domestic regulation. States argue that while principles of territorial sovereignty should be recognised to the maximum extent possible, observation of such principles may not be possible where the identity of the relevant jurisdiction is unknown.⁵² Furthermore, it may be difficult to find workable parameters for cross-border searches in unknown jurisdictions because it is not possible to consult with the interested state or request official legal assistance.

Countries have found various approaches to dealing with ‘loss of location’ in their domestic regulations. The Belgian regulation is an example of domestic law allowing for unilateral access under the Code of Criminal Procedure even if the location of the data is unknown.⁵³ There have also been discussions to explore the applicability of the principle of ubiquity that would allow for the assumption that the computer system is in the domestic jurisdiction unless it is proven that it

⁴⁹ United Nations General Assembly, *Official Compendium*, 56–57.

⁵⁰ Committee on Formation of Customary (General) International Law, *Statement of Principles Applicable to the Formation of General Customary International Law: Final Report of the Committee* (London: International Law Association, 2000), 8, www.law.umich.edu/facultyhome/drwcasebook/Documents/Documents/ILA%20Report%20on%20Formation%20of%20Customary%20International%20Law.pdf.

⁵¹ For interviews and domestic regulation examples on this topic, please see Osula, ‘Remote Search and Seizure in Domestic Criminal Procedure’, 343–373.

⁵² Law Commission, *Search and Surveillance Powers*, Report 0113-201334 97 (Wellington: New Zealand Law Commission, June 2007), www.lawcom.govt.nz/assets/Publications/Reports/NZLC-R97.pdf, 227. Explanatory Memorandum, ‘Amendments to the Criminal Code and the Code of Criminal Procedure, the Improvement and Strengthening of the Detection and Prosecution of Cybercrime (Cybercrime III)’, Netherlands, 36, www.internetconsultatie.nl/computercriminaliteit/document/727.

⁵³ Code d’Instruction Criminelle (Belgium Code of Criminal Procedure), Art. 88ter.

is not, and therefore offering a solution to the ‘loss of location’ issue.⁵⁴ Similarly, the US has amended Rule 41 of the Federal Rules of Criminal Procedure in a way that would allow a judge to issue warrants to gain ‘remote access’ to computers ‘located within or outside that district’ in cases in which the ‘district where the media or information is located has been concealed through technological means’, that is, with a possibly extraterritorial reach.⁵⁵ The amendments were target to a fair amount of criticism,⁵⁶ cautioning that such cross-border access might result in serious diplomatic consequences, ‘with short-term FBI [Federal Bureau of Investigation] investigations undermining the long-term international relationship building of the US State Department’ and possible quick escalation of responses.⁵⁷

While the amendments to the Federal Rules of Criminal Procedure specifically target investigative measures such as search and seizure (of data which may reside also in, e.g., private servers), the US CLOUD Act focuses on the government’s access to data residing at the service providers’ premises. Importantly, the US CLOUD Act includes provisions that specifically disregard the location of the data and outlines obligations that apply ‘regardless of whether such communication, record, or other information is located within or outside of the United States’.⁵⁸ Similarly, the e-Evidence EU Directive and Regulation (as will be discussed in Section 2.3.2.1) both apply to service providers ‘offering services’ in the Union or a member state, and neither the Directive nor the Regulation focuses on the location of the data in question.

Even if we employ the territoriality principle and focus on the location of data as the basis for the interpretation and prescription of jurisdiction to enforce, we can observe that the rapid technological development and need to counter sophisticated transnational crime is on the verge of making such arguments less relevant for modern states, fundamentally reshaping these concepts and interpretations. Indeed, given the changed nature of threats and virtual investigations, we can observe state practice moving in the direction of establishing legal grounds under domestic law for conducting remote search and seizure of data in circumstances where the location of the data cannot be determined⁵⁹ or when criminals ‘hide’ in ‘offshore servers’.⁶⁰ This leads us to the same conclusion as de Hert who suggested that today’s legal assessment on the territorial scope of jurisdiction to enforce should not be based on a court decision adopted some ninety years ago.⁶¹

⁵⁴ Interview with Mr Lodewijk van Zwieten, at the time of the interview serving as the Dutch Cyber Crime Prosecutor (28 May 2015).

⁵⁵ The previous wording of Rule 41 entailed a territorial limitation to the locations within the district. See Current Rules of Practice & Procedure, Criminal Rules 4, 41 and 45, Redline of Amended Rules, Including Committee Notes (*United States Courts*), 10–14, www.uscourts.gov/file/21315/download.

⁵⁶ E.g., Access Now et al., Rule 41 Coalition Letter, Electronic Frontier Foundation, 21 June 2016, www.eff.org/files/2016/06/20/rule_41_coalition_letter.pdf; Rainey Reitman, ‘With Rule 41, Little-Known Committee Proposes to Grant New Hacking Powers to the Government’, Electronic Frontier Foundation, 30 April 2016, www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government; Ailanthus, ‘Day of Action: Stop the Changes to Rule 41’, Tor Project, 21 June 2016, <https://blog.torproject.org/day-action-stop-changes-rule-41/> inviting the US Congress to support the Stop Mass Hacking Act.

⁵⁷ Ed Pilkington, ‘FBI Demands New Powers to Hack into Computers and Carry Out Surveillance’, *Guardian*, 29 October 2014, www.theguardian.com/us-news/2014/oct/29/fbi-powers-hacking-computers-surveillance; Richard M. Thompson II, *Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure*, CRS Report (Washington, DC: Congressional Research Service, 8 September 2016), www.fas.org/sgp/crs/misc/R44547.pdf.

⁵⁸ Summary for S.2383, ‘Clarifying Lawful Overseas Use of Data Act S.2383’, 2 June 2018, www.congress.gov/bill/115th-congress/senate-bill/2383.

⁵⁹ This condition would, however, also raise the question of the threshold of efforts that the law enforcement needs to invest to the attempts to identify the location before being able to declare complete loss of location.

⁶⁰ *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 21.

⁶¹ De Hert, ‘Cybercrime and Jurisdiction’, 72.

However, there is no consensus on this yet. There are also opposing views maintaining that a state's mere inability to determine the location of the data at the moment of the access 'does not mitigate the wrong caused to the affected state of a breach of territorial integrity'.⁶² These circumstances have also been compared to a situation where 'a state is not likely to accept that another state can arrest a fugitive present on the former's territory just because the former did not know of the fugitive's whereabouts'.⁶³

However, this would not mean that the concept of 'territorial sovereignty' would become less crucial in other aspects of international law. Instead, it would imply that future state behaviour will continue to shape the territorial limits of jurisdiction to enforce, outlining the exceptional circumstances for accessing digital evidence that would preclude the wrongfulness of activities that could otherwise be considered a breach of other states' sovereignty.⁶⁴ These conclusions are supported by the interviews conducted with practitioners suggesting that the criterion of 'location' is outdated,⁶⁵ and that countries should join forces in agreeing on the common grounds of the collection of extraterritorial evidence even if this requires the relinquishing of some amount of sovereignty.⁶⁶ There may also be a dissonance between publicly shared investigative measures and actual investigative practice.

The traditional scope of jurisdiction to enforce and its territorial application is and should be evolving in time in order to best fit the requirements of law enforcement and to avoid impunity for criminals. A common understanding regarding the accepted territorial scope of jurisdiction to enforce is that it should be developed by states through state practice and legal frameworks which offer both certainty and transparency for the stakeholders involved in cross-border investigation. The mentioned work of the Internet & Jurisdiction Policy Network's Data & Jurisdiction workstream is aimed towards creating one such framework, and there is a building momentum of a move towards a focus on investigate jurisdiction as introduced here.

2.2.5 *Single-Factor Test versus Multi-Factor Tests*

Regardless of what broad framework one favours, it is essential to map out what jurisdictional anchor points may be relied upon to establish a jurisdictional claim. When it comes to finding jurisdictional tests for when law enforcement may access cross-border data, a wide range of single-factor tests have been advanced, such as focusing on:

- the location of the data;
- the location of the suspect;
- the location of the victim;
- the nationality of the suspect;
- the nationality of the victim;
- the habitual residence of the suspect;
- the habitual residence of the victim;

⁶² Koops and Goodwin, *Cyberspace, the Cloud*, 61–62.

⁶³ Ryngaert, *Jurisdiction in International Law*, 82.

⁶⁴ See also Osula, 'Remote Search and Seizure of Extraterritorial Data', 116.

⁶⁵ Interview with Mr Geert Schoorens, Federal Prosecutor's Office of Belgium (28 May 2015), conducted by Anna-Maria Osula.

⁶⁶ Interview with Mr Lodewijk van Zwielen, conducted by Anna-Maria Osula.

- the location of incorporation of the data holder;
- the location of a subsidiary of the data holder; or
- the data holder having a presence in the requesting state.

Unfortunately, all these single-factor tests for jurisdiction fall well short of what is needed. Consider, for example, jurisdiction based on the location of the data sought. Can we accept a system where jurisdiction, in the context of cross-border access to data by law enforcement, always and only is based on the location of the data? The answer is obviously in the negative. There are numerous reasons for this, however; for one, as already noted, law enforcement may not always be able to identify the location of the data within a reasonable time frame.

Could we, as further examples, accept a system where jurisdiction always and only is based on either solely the nationality, or solely the location, of the person investigated? The obvious answer is again in the negative, and again there are numerous reasons for that conclusion. Perhaps most obviously, imagine that Belgian law enforcement is investigating a murder that occurred in Belgium, involving a Belgian victim and a Belgian offender. Imagine further that the relevant evidence is stored in Belgium by a Belgian private party. Would we then want law enforcement to be refused access on the basis that the offender happens to live (and be located) in the Netherlands? Or, with all other factors remaining the same, if the offender is a Dutch citizen living in Belgium, would we want law enforcement to be refused access on the basis that the offender happens to have a passport issued in the Netherlands?

Accepting the above, the only realistic option left on the table is a multi-factor test for jurisdiction in law enforcement cross-border access to data. Thus, the fruitless search for a single-factor test should be abandoned and efforts should be put towards identifying a sensible multi-factor test.

Critics of a multi-factor test may express concerns about the complexity of applying such a test and how such a test may be misused. However, first, the law is replete with multi-factor tests, and the legal community – and in fact the community more broadly – applies multi-factor tests on a daily basis. Second, the simple reality is that law cannot be drafted in a manner that excludes the risk that it is misused or abused – any legal rule may be misused. If the choice is between, on the one hand, a single-factor test that does not work and, on the other hand, a multi-factor test that more easily can be misused, surely the prudent path forward is to embrace the multi-factor test and work towards minimising the instances of its misuse (e.g., through appropriate mechanisms for appeals)?

2.2.6 *When Regulatory Compliance Is Impossible*

As already alluded to, cloud service providers may find themselves ‘between a rock and a hard place’, as the saying goes. To understand the environment in which cloud providers operate, we may usefully adopt a perspective examining what we can call their ‘contextual legal system’, by which we refer to the system of all the legal rules that purport to apply to the conduct of the cloud provider in the context of a given activity.⁶⁷ Where a cloud provider is active in multiple jurisdictions, that contextual legal system may contain conflicting obligations. This may even prompt the cloud provider to consider wilful non-compliance with the legal obligations of State A, in order to comply with those of State B. Such situations are, of course, unfruitful and harmful, and should be avoided. After all, subjectivity to the rule of law should be not an economic consideration but a universally binding principle. Where conflicting obligations

⁶⁷ Svantesson, *Solving the Internet Jurisdiction Puzzle*, 116.

cannot be eliminated, the option of providing cloud providers with immunity or other forms of protection (such as so-called clawback statutes) may be considered. This situation, in which key actors are forced to violate one state's law to comply with another's, is perhaps the single most serious normative challenge in this context.

2.3 MUTUAL LEGAL ASSISTANCE, OTHER TRADITIONAL APPROACHES AND NEW DEVELOPMENTS

Traditionally, the exchange of evidence and other information in criminal and related matters has been based on MLA. In the context of accessing extraterritorially located data, requests for mutual assistance are, in conjunction with relevant national legislation, mostly based on bilateral MLA treaties (MLATs), multilateral agreements such as the Council of Europe Convention on Cybercrime (the Budapest Convention),⁶⁸ the European Convention on Mutual Legal Assistance in Criminal Matters and other Council of Europe (CoE) treaties, United Nations (UN) and other international treaties, or reciprocity on an ad hoc or case-by-case basis.

Additionally, for complex international cases, the frameworks of Europol, Eurojust and Interpol are employed, as well as joint investigation teams and law enforcement liaison officers and networks. Such cooperation mechanisms are typically guided by the territoriality principle, which focuses, as the principal counterpart of the investigation, on the country in whose territory the data being sought resides, thereby allowing for certain transparency and having a general overview of the activities of foreign law enforcement targeting data stored on domestic territory.

While MLA has been the principal tool for accessing evidence stored extraterritorially, recent studies have indicated that these traditional means for accessing extraterritorial data may not satisfy modern criminal procedures in terms of time efficiency. In fact, it may take months for the extraterritorial evidence to reach the requesting state. For example, it has been assessed that the MLA process between the European Union and the United States takes an average of ten months.⁶⁹ Therefore, these mechanisms are considered 'too complex, lengthy and resource intensive' and are thus often abandoned.⁷⁰ The CoE's assessment of the functioning of MLA provisions concluded:

The mutual legal assistance (MLA) process is considered inefficient in general, and with respect to obtaining electronic evidence in particular. Response times to requests of six to 24 months appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the positive obligation of governments to protect society and individuals against cyber-crime and other crime involving electronic evidence.⁷¹

⁶⁸ Council of Europe, *Convention on Cybercrime*, ETS No. 185, 23 November 2001.

⁶⁹ Commission Staff Working Document Impact Assessment, Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings, SWD/2018/118 final, 17 April 2018, 25, referring to Jennifer Daskal, 'A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right', Just Security, 8 February 2016, www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/.

⁷⁰ For a comprehensive overview, see, e.g., Council of Europe, *T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime*, T-CY(2013)17rev, 3 December 2014, 31, <https://rm.coe.int/16802e726c>.

⁷¹ Council of Europe, Cybercrime Convention Committee, *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY*, T-CY (2016)5, 16 September 2014, 9, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>.

Despite its weaknesses, there are few calls for the MLA structure to be completely abandoned. Rather, the most common calls are for it to be supplemented with a system of direct requests to data holders, and for the MLA system to be made more efficient. Work on this latter improvement is being carried out, for example, by the CoE.⁷²

Alternative options for accessing extraterritorially located data include formal or informal cooperation among different countries' law enforcement, establishing and maintaining national twenty-four/seven point-of-contact networks, sending requests directly to third parties such as service providers, accessing data that is publicly available and undertaking investigative measures (such as remote search and seizure and others) to directly access data notwithstanding its location or if the location cannot be identified. However, these mechanisms would benefit from formalised cooperation between governments and the private sector.

2.3.1 Budapest Convention

The Budapest Convention is the only international agreement specifically focusing on harmonising domestic criminal substantive law in the area of cybercrime. It provides for domestic criminal procedural law powers that are necessary for the investigation and prosecution of such offences, including those offences committed by means of a computer system, as well as collecting evidence in electronic form and setting up a specific regime of international cooperation.⁷³

Importantly, the Budapest Convention recognises that the exercise of law enforcement powers inevitably interferes with the rights and freedoms of individuals, especially privacy. Therefore, the Budapest Convention clearly underlines that the establishment, implementation and application of the powers and procedures provided for in the Convention shall be subject to all the conditions and safeguards provided for under the domestic law of each party, and thus ensures that these conditions and safeguards provide for the adequate protection of human rights and liberties.⁷⁴

The Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence was adopted by the Committee of Ministers of the Council of Europe on 17 November 2021. By May 2022, the Second Additional Protocol to the Convention on Cybercrime was opened for signatures.

While the CoE's efforts on the issue of law enforcement's access to extraterritorial data will be discussed in greater detail in Chapter 8 of this volume, a few comments are in order regarding the Convention's approach to jurisdiction. Without offering a detailed definition of jurisdiction, Article 22 outlines the main jurisdictional principles for the prosecution of the offences listed in the Convention. While also mentioning other bases for jurisdiction such as the principle of nationality, the Convention's focus is on the principle of territoriality, stating that parties are not allowed to enter a reservation with respect to the establishment of territorial jurisdiction (Article 22(2)). Neither are parties allowed to enter a reservation regarding the obligation to establish jurisdiction in cases falling under the principle of *aut dedere aut judicare* (extradite or prosecute) where that party has refused to extradite the alleged offender on the basis of his/her nationality and the offender is present on its territory.⁷⁵ Importantly, the aforementioned basis for

⁷² Council of Europe, 'MLA Council of Europe Standards', www.coe.int/en/web/transnational-criminal-justice-pcoe/mla-council-of-europe-standards.

⁷³ Explanatory Report to the Convention on Cybercrime.

⁷⁴ *Ibid.*, 145.

⁷⁵ Explanatory Report to the Convention on Cybercrime, 237.

jurisdiction is not exclusive as the Convention permits the parties to establish, in conformity with their domestic law, other types of criminal jurisdiction (Article 22(4)). However, as will be explained later, the focus on territoriality (such as the location of the data as the main connecting criterion) is shifting in light of other ongoing international initiatives. For the purposes of this chapter, we will briefly discuss now only the articles related to MLA and transborder data access, and not focus on other options for accessing data stored abroad.

Article 31 is one of the principal legal constructs informing parties about options to access, under mutual assistance, data stored extraterritorially. It allows for requests to ‘search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29’ (Article 31, para. 1). For cybercrime investigations, the provision also allows requests for such assistance on an expedited basis where ‘there are grounds to believe that relevant data is particularly vulnerable to loss or modification’ or where there are other legal grounds for providing for expedited cooperation (Article 31, para. 3). Unfortunately, there are currently no statistics on the frequency of use of mutual assistance to access stored computer data among the parties to the Budapest Convention. One of the main reasons for this is the increasingly decentralised nature of MLA where a growing number of requests are sent or received directly between relevant judicial authorities and not only via central authorities.⁷⁶ Yet, the CoE has concluded that the Budapest Convention’s parties appear not to be making full use of the range of opportunities offered by the Convention and other specific agreements.⁷⁷ Therefore, the CoE issued a set of recommendations for both parties and other relevant entities on how to improve the MLA system in the context of accessing stored computer data.⁷⁸ Further, the Second Additional Protocol to the Convention on Cybercrime – specifically Articles 9 and 10 – enhances the mechanisms for accessing certain types of data in emergency situations.

As an ‘exception to the principle of territoriality’,⁷⁹ Article 32 of the Budapest Convention is not bound by the domestic territory of the party initiating criminal proceedings. The provision regulates extraterritorial access to stored computer data with consent or where publicly available, neither option requiring any additional authorisation from the other party. Article 32(b) allows a party to ‘access or receive through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system’. Unlike Article 32(a), Article 32(b) continues to be subject to debate. In addition to sovereignty-related doubts regarding the permissibility of such a clause under international law at all,⁸⁰ there are a number of concerns regarding its interpretation.

First, it appears problematic that the provision allows access only to ‘stored computer data located in another Party’. Article 32(b) would not cover situations where the location of the data is unknown, or when it is determined that the data is located in the territory of a country that is not a party to the Convention – presumably due to the assumption that

⁷⁶ Council of Europe, *T-CY Assessment Report*, 6.

⁷⁷ Ibid., 123. For further explanation, see Anna-Maria Osula, ‘Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data’ (2015) 9(1) *Masaryk University Journal of Law and Technology* 43–64.

⁷⁸ Peter Swire and Justin Hemmings, ‘Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program’ (2017) 71 *NYU Annual Survey of American Law* 687.

⁷⁹ Council of Europe, *T-CY Guidance Note #3: Transborder Access to Data (Article 32)*, 3 December 2014, 3.

⁸⁰ Marco Gercke, *Understanding Cybercrime: Phenomena, Challenge and Legal Response* (Geneva: International Telecommunication Union, 2012), 277–278, www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf. See also Russia refusing to sign the CoCC due to this clause in Keir Giles, ‘Russia’s Public Stance on Cyberspace Issues’, 2012 4th International Conference on Cyber Conflict, 5–8 June 2012, 67.

such access would require an additional threshold for determining the level of certainty required for *loss of location* or further legal basis such as the consent of the state in which the data is located. However, such a rigid interpretation of Article 32(b) renders it rather impractical for use in the investigation of transnational cybercrime where, in practice, it is not common that during an investigation, when needing to access data extraterritorially, a difference would be made between countries that are parties to the Convention and those that are not. The CoE advises, without being able to offer a concrete solution, that in situations of loss of location, parties ‘evaluate themselves the legitimacy of a search or other type of access in the light of domestic law, relevant international law principles or considerations of international relations’.⁸¹

Second, there is a debate regarding who has the ‘lawful authority to disclose the data’.⁸² In this regard, the CoE remains relatively silent, except to confirm that the ‘lawful authority’ or being ‘lawfully authorised’ to disclose data may vary depending on specific circumstances, the nature of the person and the applicable law concerned.⁸³ In particular, there are controversies regarding the interpretation of service providers acting as a ‘lawful authority’ in disclosing data to law enforcement. The CoE has been reluctant to confirm that service providers would be able to ‘consent validly and voluntarily to disclosure of their users’ data under Article 32 since service providers will only be holders of such data; they will not control or own the data, and they will, therefore, not be in a position validly to consent’.⁸⁴

The debate regarding the issues surrounding law enforcement’s requests to service providers is, of course, much greater and has come to focus on whether law enforcement has the power to request data from either a foreign service provider (established or headquartered in a foreign country) or a local service provider (established on domestic soil), in case the data is physically stored in a foreign territory, and whether there is an obligation for the service provider to respond to such requests at all. The unstable connection between the location of the data and the entity having the ‘lawful authority’ to provide access to such data is exemplified by cases where large international companies have data centres all over the world. As will be explained in Section 2.3.2.1, the EU has taken a strong stance on this question and largely abandoned the traditional territoriality-centred focus on relying only on the MLA system.

Third, the term ‘consent’ is not understood in exactly the same way in all legal systems. In many countries, cooperation in a criminal investigation would require explicit consent; however, the general agreement by an individual to the terms and conditions of an online service might not constitute explicit consent even if the provisions of the terms and conditions indicate that data may be shared with law enforcement.⁸⁵ The meaning of

⁸¹ T-CY Guidance Note #3, 3.2.

⁸² See generally about the arguments regarding lawful authority and consent in preparation of the CoE Guidance Note on Transborder Access in Micheál O’Floinn, ‘It Wasn’t All White Light Before Prism: Law Enforcement Practices in Gathering Data Abroad, and Proposals for Further Transnational Access at the Council of Europe’ (2013) 29(5) *Computer Law & Security Review*, 610, 611–613.

⁸³ An example is brought of a situation where a person’s email is stored by him/herself or by the service provider in another country, and in that case the person would have a lawful authority to disclose the data to law enforcement to permit access to the data. Explanatory Report to the Convention on Cybercrime, 294.

⁸⁴ T-CY Guidance Note #3, 3.6. Article 29 Working Party supported this approach by noting that private entities serving as data controllers cannot lawfully provide access or disclose the data to foreign LEAs that operate under a different legal and procedural framework from both a data protection and a criminal procedural point of view. Article 29 Working Party, ‘Article 29 Working Party’s Comments on the Issue of Direct Access by Third Countries’ Law Enforcement Authorities to Data Stored in Other Jurisdiction, as Proposed in the Draft Elements for an Additional Protocol to the Budapest Convention on Cybercrime’, 5 December 2013, 3, https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf.

⁸⁵ T-CY Guidance Note #3, 3.4.

‘voluntary’ may also raise questions. For example, the EU Data Protection Regulation 2016/679 warns that ‘consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment’.⁸⁶ Moreover, in practice, the requirement of obtaining consent may not be tenable in extremely time-sensitive situations, or desirable as it may prove to be detrimental to the success of the criminal investigation. Also, if the suspect does give explicit consent for remote access to his/her online accounts, law enforcement would probably proceed despite the fact that the country on whose territory the data is located is not a party to the Budapest Convention. This last point underscores again the question of how to balance the protection of sovereignty with the protection of individual rights.

Even though the aim of Article 32(b) – to provide investigatory access to evidence – is certainly justified by the practical needs of today’s law enforcement, the legal construct of the provision contains a number of issues that preclude parties from effective implementation. The CoE has attempted to clarify the exact meaning of the terms and concepts put forward in the clause, but has also finally concluded that Article 32(b) offers ‘very limited possibilities’.⁸⁷ Furthermore, the CoE notes that, in the absence of a clear and feasible international legal framework, governments have increasingly pursued unilateral solutions with risks for international relations and the rights of individuals.⁸⁸

In 2017, the CoE Cloud Evidence Group recommended starting negotiation of an Additional Protocol to the Budapest Convention. The aim would be to ‘allow for more effective MLA, to facilitate direct cooperation with service providers in other jurisdictions when needed and subject to conditions and safeguards, to frame and establish conditions and safeguards regarding existing practices of transborder access to data and to establish data protection requirements’.⁸⁹

In addition to what has been noted already, the Second Additional Protocol to the Convention on Cybercrime introduces structures for cross-border requests in Articles 6, 7 and 8. Article 6 relates to requests for domain name registration information, while Article 7 relates to disclosure of subscriber information. Article 8 regulates situations where a state is giving effect to orders from another state (that also is a party to the arrangement) for expedited production of subscriber information and traffic data.

From the perspective of jurisdiction and sovereignty, it is important to note that, in all these provisions, a territoriality focus is maintained in the sense that the provisions describe what a state should do in relation to a service provider in the territory of a party to the arrangement. Importantly, however, no weight is seemingly attached to the location of the data. Instead, focus is placed on a service provider having ‘possession’ or ‘control’ over the requested data. Put simply, states are required to regulate the service providers on their territory (territoriality in a sense), and can regulate those services providers in relation to data that they possess or control (a step away from territoriality).

⁸⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), [2016], 4 May 2016, p. 42.

⁸⁷ Council of Europe, *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY*, 44.

⁸⁸ Council of Europe, *Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY*, T-CY (2014) 16, 3 December 2014, 7–8.

⁸⁹ Council of Europe, *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY*, 40.

2.3.2 European Union Initiatives

In the EU, mutual assistance for criminal matters has been largely built upon the framework of the CoE Convention on Mutual Assistance in Criminal Matters, parts of the Schengen Convention and the EU Convention on Mutual Assistance in Criminal Matters and its Protocol. Notably, in 2014 the EU adopted Directive 2014/41/EU regarding the European Investigation Order in criminal matters,⁹⁰ which outlines a framework for a judicial authority of one member state to ‘have one or several specific investigative measure(s) carried out in another Member State’ in order to obtain evidence.⁹¹ For requests outside of the EU, MLAs are usually used.

2.3.2.1 Working around the Territoriality Principle: The New EU Legal Framework on e-Evidence

For an even more expedited process for cross-border access to digital evidence, the European Commission proposed an important legislative package called ‘e-Evidence’ on 17 April 2018.⁹² The e-Evidence legislative package included a Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings and a Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters,⁹³ which must be read together. These instruments were advanced to address a significant issue, namely, to make it easier and faster for LEAs and judicial authorities to obtain electronic evidence that is often held by foreign internet companies. While unveiled in April 2018, these proposals were preceded by a considerable period of consultations.

After long and difficult negotiations, this legislative package was finally adopted in 2023.⁹⁴ While the Directive ‘lays down rules on the legal representation in the Union of certain service providers for receipt of, compliance with and enforcement of decisions and orders issued by competent authorities of the Member States for the purposes of gathering evidence in criminal proceedings’,⁹⁵ the Regulation ‘lays down the rules under

⁹⁰ Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in Criminal Matters [2014] OJ L 130, 1 May 2014.

⁹¹ Importantly, as of 22 May 2017, this Directive replaced most of the existing laws in the area of transferring evidence between member states in criminal cases. Directive 2014/41/EU, Art. 1(1).

⁹² These proposals have been discussed in detail in, e.g., Stanisław Tosza, ‘The European Commission’s Proposal on Cross-Border Access to e-Evidence: Overview and Critical Remarks’ (2018) 4 *Eucrim* 212–219; Mark D. Cole and Teresa Quintel, ‘Transborder Access to e-Evidence by Law Enforcement Agencies’, University of Luxembourg Law Working Paper 2018-010, 2018, <http://dx.doi.org/10.2139/ssrn.3278780>; Vanessa Franssen, ‘The European Commission’s e-Evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?’, *European Law Blog*, 12 October 2018, <https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/>.

⁹³ European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters, COM/2018/225 final – 2018/0108 (COD), 17 April 2018; European Commission, Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings COM/2018/226 final – 2018/0107 (COD), 17 April 2018.

⁹⁴ See also Chapter 7 in this volume.

⁹⁵ Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (Legal Representative’s Directive) [2023] OJ L 191/181 (e-Evidence Directive), Art. 1(1).

which an authority of a Member State may order a service provider offering services in the Union, to produce or preserve electronic evidence, regardless of the location of data'.⁹⁶

To understand how the new legal framework will impact actors outside the EU, there are some key concepts that must be understood. First, the definition of the types of service provider caught by these instruments includes any natural or legal person that provides one or more of several types of services, including 'internet domain name and IP [internet protocol] numbering services such as IP address assignment, domain name registry, domain name registrar and domain name-related privacy and proxy services',⁹⁷ certain electronic communications services,⁹⁸ as well as 'other information society services ... that (i) enable their users to communicate with each other; or (ii) make it possible to store or otherwise process data on behalf of the users to whom the service is provided, provided that the storage of data is a defining component of the service provided to the user'.⁹⁹ Essentially, the scope of which types of service provider fall within the arrangement is broad, and may not fully address the current issues with the third country service providers.

The next concept that must be understood is the jurisdictional scope. In order to accomplish this, we need to start with the observation that both the Directive and the Regulation apply to service providers 'offering services' in the Union or a member state.¹⁰⁰ While this may seem relatively specific, 'offering services' in a member state (or in the Union) means enabling legal or natural persons in a member state to use the service and 'having a substantial connection to the Member State' in question.¹⁰¹ An examination of Recital 11 of the Legal Representative's Directive and Recital 30 of the e-Evidence Regulation then further clarifies that a 'substantial connection' does not need to be particularly substantial at all. Rather, a substantial connection to the Union exists

- (1) where the service provider has an establishment in the Union; or
- (2) where the service provider does not have an establishment in the Union, but the service provider:
 - (a) has a significant number of users in one or more Member States;
 - (b) is targeting its activities towards one or more Member States; or
 - (c) directs its activities towards one or more Member States as set out in Article 17(1)(c) of Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.¹⁰²

Thus, this new legal framework entails a targeting test that incorporates all the uncertainties, blemishes and warts, typical of a targeting test, and that clearly has the potential to cater for far-reaching jurisdictional claims and has little to do with any truly 'substantial connection'. Additionally, it is interesting to note the odd double use of the targeting test, first as a stand-alone

⁹⁶ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (e-Evidence Regulation) [2023] OJ L 191/118, Art. 1(1).

⁹⁷ e-Evidence Directive, Art. 2(1)(b) and e-Evidence Regulation, Art. 3(3)(b).

⁹⁸ e-Evidence Directive, Art. 2(1)(a) and e-Evidence Regulation, Art. 3(3)(a).

⁹⁹ e-Evidence Directive, Art. 2(1)(c) and e-Evidence Regulation, Art. 3(3)(c).

¹⁰⁰ e-Evidence Directive, Art. 1(5) and e-Evidence Regulation, Art. 1(1).

¹⁰¹ e-Evidence Directive, Art. 2(2)(a) and e-Evidence Regulation, Art. 3(4)(b).

¹⁰² Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), [2012] OJ L 351, 20 December 2012.

measure specifically described as ‘targeting’ (see (2)(b) in the structure above) and then targeting as articulated in the context of Article 17(1)(c) of Regulation 1215/2012 (see (2)(c) in the structure above).¹⁰³

With regard to the former targeting test, the aforementioned Recitals 11 and 30 explain that

[t]he targeting of activities towards one or more Member States should be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering goods or services. The targeting of activities towards a Member State could also be derived from the availability of an application (‘app’) in the relevant national app store, from the provision of local advertising or advertising in the language used in that Member State, or from the handling of customer relations, such as by the provision of customer service in the language generally used in that Member State.

While there are some additional examples included (e.g., the reference to the relevant national app store), this explanation is the same targeting test as that of Article 17(1)(c) of Regulation 1215/2012. This double use of ‘targeting’ is a potential source of confusion. As a consequence, the wording of the Legal Representative’s Directive and the e-Evidence Regulation fails to limit the jurisdictional reach of these instruments to those situations that have an actual substantial connection.¹⁰⁴ This is a disappointing outcome particularly in light of the fact that the drafters were on the right path, as they did specify the requirement of a ‘substantial connection’.

Despite this, the EU legislator is addressing the investigator’s legitimate interests¹⁰⁵ and has, for example, sought to limit the types of crime in relation to which the measures in question may be taken.¹⁰⁶ It is also encouraging to see that a sophisticated balancing of interests is a clearly articulated aspect of these instruments.¹⁰⁷ This is particularly so in relation to Article 17 of the e-Evidence Regulation, which aims ‘[t]o ensure comity with respect to the sovereign interests of third countries, to protect the individual concerned and to address conflicting obligations on service providers’ by providing ‘a specific mechanism for judicial review’ in cases of clashes with legal obligation stemming from the law of third states.¹⁰⁸ This provision instructs the court to engage in an interest balancing exercise, ‘weighing a number of elements which are designed to ascertain the strength of the connection to either of the two jurisdictions involved, the respective interests in obtaining or instead preventing disclosure of the data, and the possible consequences for the addressee or for the service provider of complying with the order’.¹⁰⁹ To conclude, while these new instruments contain several good elements, the application of the ‘substantial connection test’ will likely raise questions in the future.

2.3.2.2 Addressing the International Dimension

In parallel to the discussions on the e-Evidence package, the European Council concluded in October 2018 that ‘solutions should be found to ensure swift and efficient cross-border access to e-evidence in order to effectively fight terrorism and other serious and organised crime, both

¹⁰³ See, e.g., Case C-585/08, *Pammer v. Reederei Karl Schlüter GmbH & KG* and Case C-144/09 *Hotel Alpenhof GesmbH v. Oliver Heller*, 7 December 2010.

¹⁰⁴ Internet & Jurisdiction Policy Network, *Data & Jurisdiction Program: Operational Approaches, Norms, Criteria, Mechanisms*, April 2019, 31–32, www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Program-Operational-Approaches.pdf.

¹⁰⁵ *Ibid.*

¹⁰⁶ See, e.g., e-Evidence Regulation, Art. 5(4).

¹⁰⁷ Regarding the need for this, see, e.g., *Data & Jurisdiction Program*, 31–32.

¹⁰⁸ e-Evidence Regulation, Recital 74.

¹⁰⁹ *Ibid.*, Recital 78. See also e-Evidence Regulation, Art. 17(6).

within the EU and at international level’ and that the Commission should ‘urgently submit negotiating mandates for the international negotiations on e-evidence’.¹¹⁰ In response, the Commission presented two negotiating mandates which were adopted by the Council.¹¹¹

The first mandate focuses on the negotiations with the US in order to address the challenge of US service providers not always being allowed to, or for other reasons being reluctant to, directly cooperate with European LEAs. Specifically, the mandate includes the goal of reaching an agreement on timely access to electronic evidence by shortening the time period for supplying the requested data to ten days; avoiding possible legal conflicts by setting out definitions and types of data covered, clarifying legal obligations and ensuring reciprocal rights for all parties; as well as guaranteeing strong safeguards on data protection, privacy and procedural rights.

The second mandate allows starting negotiations on behalf of all the member states on the now concluded Second Additional Protocol to the Budapest Convention. These negotiations focused on, inter alia, the compatibility of the Protocol with current and future EU law (which was challenging, considering that the negotiations on the e-Evidence package had not yet been concluded when the Protocol was being drafted), enhanced international cooperation through more effective MLA, direct cooperation of law enforcement with service providers in other jurisdictions, and stronger safeguards for the protection of personal data and national practices.

Overall, these initiatives are a clear sign of the acknowledged need to ensure that the acquisition of e-evidence remains compliant with the requirements deriving from international law and an indication of the potential role of the principle of territoriality in designing the legal tools for cross-border access to data. It is also worth pointing out that these mandates partly reflect the criticism that the EU Commission received in response to its proposed e-Evidence package. For example, the European Parliament expressed concerns about a number of serious legal questions related to the proposed package, such as the extraterritorial reach of EU law, proportionality, the relationship of the proposed instrument to the provisions and the Protocols of the Budapest Convention, data protection implications and procedural safeguards such as the notification¹¹² requirement.¹¹³ While the result of the second mandate is by now well-known, the negotiations with the US on a future ‘CLOUD Act’ agreement (see Section 2.3.3) are still ongoing at the time of writing.

2.3.3 *The US CLOUD Act*

The US currently plays a central role in the context of LEAs accessing digital evidence due to the fact that most of the data sought as evidence is held by US companies. The centrality of the US

¹¹⁰ European Council, *Conclusions*, EUCO 13/18, 18 October 2018, www.consilium.europa.eu/media/36775/18-euco-final-conclusions-en.pdf.

¹¹¹ Council of the European Union, *Council Decision on Authorising the Opening of Negotiations with a View to Concluding an Agreement between the European Union and the United States of America on Cross-Border Access to Electronic Evidence for Judicial Cooperation in Criminal Matters*, 9114/19, 21 May 2019, <https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/en/pdf>; Council of the European Union, *Council Decision on Authorising the European Commission to Participate, on Behalf of the European Union, in Negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime* (CETS No. 185), 9116/19, 21 May 2019, <https://data.consilium.europa.eu/doc/document/ST-9116-2019-INIT/en/pdf>.

¹¹² Anna-Maria Osula and Mark Zoetekouw, ‘The Notification Requirement in Transborder Remote Search and Seizure: Domestic and International Law Perspectives’ (2017) 11(1) *Masaryk University Journal of Law and Technology* 103–128.

¹¹³ European Parliament, *Committee on Civil Liberties, Justice and Home Affairs, Working Document on the Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters – Introduction and Overall Assessment of Issues* (2018/0108 (COD)), PE631.925v02-00, 7 December 2018, www.euro-parl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-631.925&format=PDF&language=EN&secondRef=02.

position is such that it has prompted some US scholars to adopt the perspective that legal assistance may be analogous to the visa waiver system:

Historically, each foreign visitor to the United States required an in-person interview with a U.S. consular official. As the volume of business and tourist visits to the United States increased enormously, that sort of case-by-case interview became a barrier to international travel as well as a bad use of scarce consular resources. Today, 41 countries have qualified under the clear criteria for the VWP, so that the vast majority of visitors from those countries can enter the United States without the individualised interview previously required.

Applied in the MLA context, due to the analogous globalisation of cross-border evidence, eligible countries with high-quality procedures for seeking evidence would be eligible for a streamlined process for obtaining evidence in the United States.¹¹⁴

Any initial appeal of such a comparison evaporates on a sober-minded analysis of the actual state of things. Under a visa waiver arrangement, the countries benefiting from the scheme lack rights to the benefits to be had and they lack means to obtain what they want outside the visa waiver arrangement. In contrast, when it comes to law enforcement access to data, the countries wanting the data in question may argue that they, indeed, have a right to request the data. Further, they have alternative means to access the data ('hacking' in the worst case), and there are third parties (the technology companies holding the data) that may be squeezed in the middle where there is a clash. Consequently, despite US-centric sentiments among some US academics,¹¹⁵ we are not dealing with a situation where the US can expect to make all the decisions, handing out privileges to those it wishes to favour. In any case, as the uptake of non-US online services increases, the centrality of the US is declining. Furthermore, it is perhaps possible to detect a certain fatigue among non-US law enforcement prompting unilateral actions.

The US government has itself experienced the difficulty involved in accessing evidence stored in the cloud. In December 2013, it served a search warrant on Microsoft under the Electronic Communications Privacy Act of 1986 (ECPA). The warrant authorised the search and seizure of information associated with a specified web-based email account that is stored at premises owned, maintained, controlled or operated by Microsoft. Microsoft opposed the warrant since the relevant emails were located exclusively on servers in Dublin, Ireland. After a journey through the legal system, the matter ended up before the Supreme Court of the US. However, the case of *Microsoft Corp. v. United States*¹¹⁶ was rendered redundant by a legislative initiative.

In March 2018, the US adopted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act).¹¹⁷ At least partially driven by the controversy surrounding the dispute in *Microsoft Corp. v. United States*,¹¹⁸ the CLOUD Act was enacted with the primary function of amending the Stored Communications Act (SCA) of 1986 so as to allow federal law enforcement to compel US-based technology companies, via warrant or subpoena, to provide requested data stored on servers regardless of whether the data is stored in the US or on foreign soil – a clear step away from strict territoriality focused on the location of data. This is combined with a mechanism for managing the risk of conflicts with foreign law such as that which arose in the *Microsoft Warrant* case. More precisely, the CLOUD Act includes 'a new statutory basis for providers to move to quash based on a conflict with foreign law, albeit only in those limited circumstances in which

¹¹⁴ Swire and Hemmings, 'Mutual Legal Assistance', 687, 690.

¹¹⁵ *Ibid.*, 690.

¹¹⁶ *United States v. Microsoft Corp.*

¹¹⁷ See also Chapter 21 in this volume.

¹¹⁸ *United States v. Microsoft Corp.*

the conflict is with a “qualifying foreign government” [see later] and the United States seeks the data of a non-U.S. person located outside the United States’.¹¹⁹

The CLOUD Act also gives the US government the possibility to conclude bilateral agreements with ‘qualifying foreign governments’ on data sharing, which would provide partners direct access to personal data stored in the US. To qualify, foreign governments would need to be certified by the US Attorney General, and meet certain human rights standards defined in the Act. Numerous restrictions also apply. For example, as noted by Daskal, ‘partner foreign governments can directly access foreigners’ data and hence set the rules, albeit with a number of baseline requirements in place, concerning access to that data. But if they want access to U.S. citizen and resident data, they still need to get U.S. court approval based on the U.S. standard of probable cause.’¹²⁰ At the time of writing, the UK¹²¹ and Australia¹²² have entered into the arrangements with the US anticipated under the CLOUD Act. The negotiations with the EU are still ongoing,¹²³ and so are those with Canada.¹²⁴

2.3.4 *The Internet & Jurisdiction Policy Network*

Looking outside the traditional sources for initiatives in this arena, for some years the legal issues surrounding law enforcement access to digital evidence have been a focus area of the Internet & Jurisdiction Policy Network. As one of its three Thematic Programs, the Data & Jurisdiction workstream has sought to tackle the issue of how transnational data flows and the protection of privacy can be reconciled with lawful access requirements to address crime.¹²⁵ Due to the active involvement of a broad range of stakeholders, significant progress has been made towards the development of an operational framework.¹²⁶

With developments occurring domestically (e.g., the US CLOUD Act), regionally (e.g., the EU e-Evidence package) and via international bodies (e.g., the CoE), the dialogue facilitated by, and the coordinating function of, the Internet & Jurisdiction Policy Network may prove to be highly useful.

2.4 CONCLUDING REMARKS

This chapter has outlined a number of normative challenges related to jurisdiction over data residing abroad. We have illustrated how the law enforcement process involves different types of

¹¹⁹ Jennifer Daskal, ‘Unpacking the CLOUD Act’, *Eucrim*, 31 January 2019, <https://eucrim.eu/articles/unpacking-cloud-act/>.

¹²⁰ *Ibid.*

¹²¹ Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, www.justice.gov/dag/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern-ireland. For further analysis, see Chapter 20 in this volume.

¹²² Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, www.homeaffairs.gov.au/nat-security/files/cloud-act-agreement-signed.pdf.

¹²³ US Department of Justice, ‘Justice Department and European Commission Announces [sic] Resumption of U.S. and EU Negotiations on Electronic Evidence in Criminal Investigations’, 2 March 2023, www.justice.gov/opa/pr/justice-department-and-european-commission-announces-resumption-us-and-eu-negotiations.

¹²⁴ US Department of Justice, ‘United States and Canada Welcome Negotiations of a CLOUD Act Agreement’, 22 March 2022, www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement.

¹²⁵ Internet & Jurisdiction Policy Network, ‘Data & Jurisdiction Program’, www.internetjurisdiction.net/work/data-jurisdiction.

¹²⁶ *Ibid.* See also Internet & Jurisdiction Policy Network, www.internetjurisdiction.net/data/toolkit.

jurisdictional claim and pointed to the challenges brought about in bundling investigative measures with invasive enforcement measures such as that of the *Eichmann* case. Furthermore, we have highlighted that the traditional focus on territoriality, as put forward by the *Lotus* case, does not meet the needs of law enforcement efforts in fighting cybercrime. In fact, basing the claims of jurisdiction to enforce strictly on the location of data raises several questions in terms of the threshold of breaching sovereignty and the legality of such data access under international law. We argue that ‘loss of location’ may be seen as a precluding factor in determining whether transborder access to data during an investigation entails a breach of international law. Further, we have brought attention to the inadequacies associated with single-factor jurisdictional tests and pointed to the need for multi-factor assessments. In addition, we discussed the issues associated with key actors being placed in a position where compliance with one state’s law necessitates the violation of another state’s law.

The search for possible responses to these challenges, in the chapter, then turned to analysing ongoing international initiatives attempting to solve issues related to transborder access to data. Against the backdrop of the criticism towards the MLA system, we observed a clear trend of moving away from the territoriality principle in all of the US, CoE, EU and Internet & Jurisdiction Policy Network proposals and processes. We have underlined that some of these initiatives, such as the CoE Second Additional Protocol and the e-Evidence Regulation, are still too new to be fully evaluated. However, we would like to reinforce that the legislators should ensure that legal frameworks supporting the needs of modern criminal investigations take into account the characteristics of digital evidence. This includes addressing various challenges related to digital forensics, procedural effectiveness, legislative clarity and legal safeguards as well as specialised training for law enforcement agents and judicial officers. Given the increasing need to access data that is not stored domestically, domestic legal frameworks should be clear about the conditions and limits of such investigative measures. If it is not regulated by law, or is regulated in an obscure manner, more uncertainty will be generated in respect of the application of investigative measures domestically, which may result in the routine breaching of the rights and freedoms of individuals (such as privacy, secrecy of communication, right to a fair trial), and also in relation to the legality of such state behaviour in general.

Ultimately, the challenges associated with ensuring appropriate law enforcement access to digital evidence require international cooperation and coordination. They require a degree of compromise by both LEAs and the technology industry, yet they also necessitate strict adherence to the rule of law and the protection of fundamental human rights. Further, successful solutions will not be found in blind adherence to hollow and outdated international law principles.

Much work is needed in this field and the lack of coordination is a serious obstacle for progress. There is a clear need to establish agreement around a basic framework such as the three-factor jurisprudential framework for jurisdiction that we discussed, and that has been adopted in the multi-stakeholder work of the Internet & Jurisdiction Policy Network. Only then can coordination take place in relation to the more detailed criteria for when law enforcement may gain cross-border access to electronic evidence.

Effective Data Protection and Direct Cooperation on Digital Evidence

Gavin Robinson

3.1 INTRODUCTION

Criminal investigations and proceedings substantiate and establish the innocence or guilt of a (traditionally, natural) person in respect of suspicions of criminal conduct or specified criminal charges. Accordingly, putative digital evidence sought by police and judicial authorities – whether in the domestic or in a cross-border setting – will very often qualify as personal data, defined in the EU General Data Protection Regulation (GDPR)¹ as any information

relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.²

Furthermore, chains of cooperation between private actors (for instance, ‘tech’ companies) and public authorities (classically the police, prosecutors, judges and courts) involve multiple instances of data processing, defined in the GDPR as ‘any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction’.³ In recent years, the imperative to access digital evidence (and thus personal data) has driven intense policy- and law-making activity on both sides of the Atlantic. A particular focus therein has been on streamlining the cross-border obtention of communications data from (tele)communications service providers.

The year 2018 stands out as the year which saw the passing of the CLOUD Act⁴ in the USA and the release of the European Commission’s ‘e-Evidence package’.⁵ At the time of writing the bulk of this chapter, the latter proposal remained locked in trilogue negotiations more than four years

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), [2016] OJ L 119, 4 May 2016, pp. 1–88.

² GDPR, Art. 4(1).

³ GDPR, Art. 4(2).

⁴ Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, div. V(2018) (enacted) amending various parts of Title 18 (United States Code) USC, including Chapter 121.

⁵ European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, [2018] COM(2018) 225 final, 17 April 2018 (Draft e-Evidence Regulation), https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF; European Commission, Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the

on – although the summer of 2022 heralded a breakthrough, before a final compromise text emerged in early 2023.⁶ Over at the Council of Europe, lengthy negotiations on a Second Additional Protocol (2nd Protocol) to the 2001 Cybercrime Convention (Budapest Convention)⁷ came to fruition in November 2021.⁸ Whilst those three developments differ in many important respects, they all share a gradualist (and contested) enshrinement of an enforceable legal mechanism for so-called direct cooperation across territorial borders, meaning the ‘unmediated’⁹ serving by criminal investigators (with or without prior judicial authorisation) of binding orders for the production of data in one jurisdiction on private entities based or represented in another jurisdiction – without involving or potentially even informing the relevant local authority.

Another of the mentioned reforms’ points in common tends, on the other hand, to be conspicuous by its absence from the policy debates: whilst the ongoing policy drive aims at achieving faster, more efficient and more reliable cross-border access to data, there is a dearth of specific treatment of the intertwined data protection issues.

Indeed, to the extent that data protection has entered the ‘e-evidence debate’, the greater mass of policy and scholarly attention has so far focused on the paradigmatic transatlantic cases of *Microsoft Ireland* (US investigator, data in Europe)¹⁰ and *Yahoo! Belgium* (EU member state investigator, provider and data in the USA).¹¹ The ramifications of the *Schrems*¹² jurisprudence from the Court of Justice of the European Union (CJEU) and the future of data transfers from the EU to the USA post-CLOUD Act also loom large in expert commentary.¹³ This is understandable, not least given the dominance of US-based tech companies on the EU market and the legitimate sense of urgency caused by the absence of a framework for data sharing from the EU to

purpose of gathering evidence in criminal proceedings (Legal Representatives Directive, draft LRD), [2018] COM (2018) 226 final, 17 April 2018.

⁶ As will be unpacked in Section 3.4.1.

⁷ Council of Europe, *Convention on Cybercrime* (Budapest Convention), ETS No. 185, 23 November 2001.

⁸ In May 2022, the Second Protocol was opened for signature by the Parties to the Convention; see European Union, ‘Enhanced Co-operation and Disclosure of Electronic Evidence: International Conference & Opening for Signature of the 2nd Additional Protocol to the Convention on Cybercrime’, [2022] OJ L 134, 11 May 2022, www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention.

⁹ Distinguishing ‘mediated’, ‘unmediated’ and ‘hybrid’ models of access to electronic data. See S. Carrera, G. González Fuster, E. Guild and V. Mitsilegas, ‘Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights’, *Centre for European Policy Studies*, 8 July 2015, www.ceps.eu/ceps-publications/access-electronic-data-third-country-law-enforcement-authorities-challenges-eu-rule-law/.

¹⁰ *Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016); see ‘Privacy – Stored Communications Act – Second Circuit Holds that the Government Cannot Compel an Internet Service Provider to Produce Information Stored Overseas’ (2016) 130(2) *Harvard Law Review* 769–776. On appeal, the case was vacated by the US Supreme Court as *United States v. Microsoft Corp.*, 584 US (2018) following passage of the CLOUD Act in March 2018.

¹¹ Cour de cassation (Belgian Supreme Court), 1 December 2015, P.13.2082.N. Covering both ‘Yahoo! Belgium’ and ‘Microsoft Ireland’, see P. De Hert, C. Parlar and J. Thumfart, ‘Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders: From Yahoo Belgium to Microsoft Ireland’ (2018) 9(3) *New Journal of European Criminal Law* 326–352. See also Chapter 9 in this volume.

¹² Case C-498/16 *Maximilian Schrems v. Facebook Ireland Limited* [2018] ECLI:EU:C:2018:37 (‘*Schrems I*’); Case C-311/18 *Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems* [2020] ECLI:EU:C:2020:559 (‘*Schrems II*’). See V. E. L. Cervantes, ‘The Schrems II Judgment of the Court of Justice Invalidates the EU–US Privacy Shield and Requires “Case by Case” Assessment on the Application of Standard Contractual Clauses (“SCCs”)’ (2020) 6(4) *European Data Protection Law Review* 602–606.

¹³ See P. Swire, ‘When Does GDPR Act as a Blocking Statute: The Relevance of a Lawful Basis for Transfer’, *Cross-Border Data Forum*, 4 November 2019, www.crossborderdataforum.org/when-does-gdpr-act-as-a-blocking-statute-the-relevance-of-a-lawful-basis-for-transfer. See also T. Christakis, ‘Transfer of EU Personal Data to U.S. Law Enforcement Authorities after the CLOUD Act: Is There a Conflict with the GDPR?’, in R. S. Milch, S. Benthall and A. Potcovaru (eds.), *Building Common Approaches for Cybersecurity and Privacy in a Globalized World* (New York: New York University Center for Cybersecurity, e-book, 2019), 60–75, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3508933.

the USA since the – equally legitimate, and moreover inevitable – annulment of the Privacy Shield by the CJEU in *Schrems II*.¹⁴

Yet a policy drive locked on removing legal obstacles to enforceable cross-border production orders and expert debates on the flux surrounding transatlantic data transfers risk overlooking the broader impacts of the as-yet-inchoate paradigm shift towards formalised direct cooperation on data protection standards in other ‘direct cooperation’ scenarios: namely, those involving other third states, intra-EU cases and direct cooperation in purely ‘domestic’ cases.

Indeed, even where a criminal case involving digital evidence is in all core respects – investigating authority, suspect, victims, data and third parties in control of that data – local, meaning there is no need to reach beyond the national territorial borders of one EU member state in the course of investigations, EU data protection law already comes into play. The starting point is that the stronger GDPR standards apply to the private parties called upon to cooperate with criminal investigators, and the weaker standards in the so-called Law Enforcement Directive (LED)¹⁵ – as implemented in national law – apply to the latter.

But what does the coexistence of the GDPR and the LED imply for direct cooperation on digital evidence? Does a *prima facie* neat separation between the two instruments always match the realities of private-to-public data transfers? Is the legal framework sufficiently harmonious to fully warrant description as an EU data protection *acquis*? How far can the evolving case law of the CJEU take us in illuminating blind spots, and what are the prospects for the ongoing strengthening of enforcement powers heralding greater legal certainty regarding not only the supply of digital evidence but also the applicable data protection laws, extending to meaningful, workable data subject rights? Those are the tensions, underexamined in both policy and academic debates, which this chapter aims to explore.

The chapter’s focus is on direct (‘unmediated’) *cooperation* with *third parties* in control of data pertaining to the target of investigations or proceedings – although indirect or ‘mediated’ cooperation will also be mentioned where instructive. As such, it touches only in passing on the obtention of digital evidence ‘directly’ from the target, whether in the context of consensual ‘trans-border access’ to data,¹⁶ the search and seizure of digital devices and of data,¹⁷ or so-called police hacking. At the same time, the chapter stakes no claim as to the (empirical)¹⁸ case made for the necessity of

¹⁴ In March 2022 the European Commission and the United States announced an agreement in principle on a new ‘Trans-Atlantic Data Privacy Framework’, and in October 2022 US President Biden issued an ‘Executive Order on Enhancing Safeguards for United States Intelligence Activities’ to pave the way for the establishment of a new ‘Data Protection Review Court’. At the time of writing, the Commission envisaged moving to the next steps, including proposing a draft adequacy decision and launching its adoption procedure. See European Commission, ‘Questions & Answers: EU–U.S. Data Privacy Framework’, 7 October 2022, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045.

¹⁵ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (LED), [2016] OJ L 119, 4 May 2016, pp. 89–131.

¹⁶ See, e.g., Budapest Convention, Art. 32b, pursuant. See further N. Seitz, ‘Transborder Search: A New Perspective in Law Enforcement?’ (2005) 7(1) *Yale Journal of Law & Technology* 23–50.

¹⁷ See Chapter 5, this volume. See also M. Caianiello and A. Camon (eds.), *Digital Forensic Evidence: Toward Common European Standards in Antifraud Administrative and Criminal Investigations* (Milan: Wolters Kluwer/CEDAM, 2021).

¹⁸ For a critical view, see G. G. González Fuster and S. V. Maymir, ‘Cross-Border Access to E-Evidence: Framing the Evidence’, *Centre for European Policy Studies*, 2 March 2020, www.ceps.eu/ceps-publications/cross-border-access-to-e-evidence/.

new direct cooperation powers at EU level as opposed to a less radical ‘express EIO¹⁹ for data’,²⁰ nor makes any attempt to tackle the long list of possible improvements to the mutual legal assistance (MLA) systems already in place for most cooperation beyond the Union.²¹

Especially since the endowment of the Charter of Fundamental Rights of the European Union²² with the same legal value as the Treaties,²³ it can often seem that almost every conceivable facet of a putative direct cooperation mechanism can be connected to the ‘all-overriding fundamental (super-)right²⁴ to personal data protection under its Article 8. The chapter does not aim to inventory all such issues. Data security and the related organisational and technological measures required in order to seamlessly send data between (duly authenticated²⁵) actors in the course of criminal investigations will not be addressed.²⁶ Likewise, ongoing infrastructural, practical or training efforts to (further) digitalise cross-border justice²⁷ and police cooperation²⁸ within the EU will not be seen in any detail.

The aim is rather to further the discussion on the potential impact of direct cooperation on digital evidence in criminal matters on two of the three cornerstones of EU data protection law, as enshrined in Article 16 of the Treaty on the Functioning of the European Union (TFEU) and Article 8 of the Charter: data processing principles and data subject rights.²⁹

¹⁹ The abbreviation ‘EIO’ refers to Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (EIO Directive), [2014] OJ L 130, 1 May 2014, pp. 1–36.

²⁰ See in detail in Chapter 7, this volume; and, comparing co-legislators’ positions on key elements of the reform, in K. Ligeti and G. Robinson, ‘Sword, Shield and Cloud: Toward a European System of Public–Private Orders for Electronic Evidence in Criminal Matters?’, in V. Mitsilegas and N. Vavoula (eds.), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (Oxford: Hart, 2021), ch. 2, <https://hdl.handle.net/10993/43778>.

²¹ See, e.g., S. Tosza, ‘Cross-Border Gathering of Electronic Evidence: Mutual Legal Assistance, Its Shortcomings and Remedies’, in V. Franssen and D. Flore, *Société numérique et droit pénal* (Brussels: Larcier/Bruyllant, 2019), 269–285.

²² Charter of Fundamental Rights of the European Union (Charter), [2012] OJ C 326, 26 October 2012, pp. 391–407 (Charter).

²³ Treaty on European Union (TEU), [2016] OJ C 202, 7 June 2016, Art. 6(1).

²⁴ Opinion of Advocate General Bobek in Case C-175/20, *SLA ‘SS’ v. Valsts ierēsmumu dienests*, 2 September 2021, ECLI:EU:C:2021:690, para. 2. See also, in detail, N. Purtova, ‘The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law’ (2018) 10(1) *Law, Innovation and Technology* 40–81.

²⁵ Lest, for instance, impersonators should successfully serve ‘official’ orders on unsuspecting service providers. See, e.g., W. Turton, ‘Apple and Meta Gave User Data to Hackers Who Used Forged Legal Requests’, *Bloomberg*, 30 March 2022, www.bloomberg.com/news/articles/2022-03-30/apple-meta-gave-user-data-to-hackers-who-forged-legal-requests.

²⁶ See, for instance, European Data Protection Supervisor (EDPS), ‘Opinion 7/2019 EDPS Opinion on Proposals Regarding European Production and Preservation Orders for Electronic Evidence in Criminal Matters’ (EDPS e-Evidence Opinion), 6 November 2019, paras. 33–38 insisting on the need for verification of the authenticity of certificates and orders, security of transmission of certificates and the requested data, and that provisions on identifying authorities emitting orders and legal representatives receiving them should be active before system launch in order to reduce risks of personal data breaches.

²⁷ In 2022, most member states are expected to begin using ‘e-EDES’ (the e-Evidence Digital Exchange System, European Commission) for electronic transmission of EIOs, which may be used in order to obtain digital evidence; Eurojust is also preparing to connect to and possibly use e-EDES. See Eurojust, *Annual Report 2021*, 2 March 2022, 67, www.eurojust.europa.eu/publication/annual-report-2021-20-years-criminal-justice-across-borders.

²⁸ In December 2021, the Commission proposed an EU Police Cooperation Code including a draft Directive on information exchange between the law enforcement authorities of member states, repealing the so-called Swedish Framework Decision from 2006 and a draft Regulation on automated data exchange for police cooperation (Prüm II); see the press release from the European Commission, ‘Boosting Police Cooperation across Borders for Enhanced Security’, 8 December 2021, https://home-affairs.ec.europa.eu/news/boosting-police-cooperation-across-borders-enhanced-security-2021-12-08_en.

²⁹ The third cornerstone, independent supervision, is largely left to future research efforts. See P. De Hert and J. Sajfert, ‘The Role of the Data Protection Authorities in Supervising Police and Criminal Justice Authorities Processing Personal Data’, in C. Brière and A. Weyembergh (eds.), *The Needed Balances in EU Criminal Law: Past, Present and Future* (Oxford: Hart, 2018), 250.

As both of these interrelated foundations of EU data protection law flow from the applicable rules, that is where the analysis begins in Section 3.2, with a presentation of the main plinths of the current EU legal framework. Thereafter, the interactions between that legal framework and direct public–private cooperation on digital evidence are explored in Section 3.3, before the significance from a data protection perspective of ongoing reforms at EU and Council of Europe level is discerned in Section 3.4. Section 3.5 offers some concluding remarks.

3.2 MAIN PLINTHS OF THE EU DATA PROTECTION ACQUIS

Although in 2009 the Lisbon Treaty, in collapsing the pillars of the Union, brought a new horizontal legal basis for data protection in Article 16 TFEU and elevated the right to data protection in the Charter to constitutional level,³⁰ the political rider in Declaration No. 21 to the Lisbon Treaty concerning the fields of judicial cooperation in criminal matters and police cooperation already hinted that the next generation of EU legislation on data protection was to retain some level of ‘pillarisation’³¹ well into the future, owing to the ‘specific nature’ of those two fields.³²

So it materialised, with the GDPR thus now in place for service providers’ handling of customers’ personal data,³³ and the LED applying to the ‘processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security’.³⁴

Therefore, whenever data is transferred by private actors to the competent authorities, a priori this entails a switch of data protection regime: the data ‘travels’ from the GDPR regime to the LED regime as implemented in national law. Whether and to what extent this is always the case in different scenarios of public–private cooperation will be examined in greater detail in Section 3.3. First, however, it is necessary to prepare the ground with a brief comparison of the scope and levels of protection offered by each legal instrument.

3.2.1 *The GDPR and ePrivacy Reform*

Pursuant to Article 2(2) of the GDPR, the Regulation does not apply to four types of personal data processing, two of which are most relevant for present purposes: processing in the course of an activity which falls outside the scope of Union law (Article 2(2)(a)) and processing ‘by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security’ (Article 2(2)(d)). This exception thus mirrors word-for-word the material scope of its sister instrument, the LED, as set out in Section 3.2. The GDPR does apply, however, when competent authorities process personal data for purposes other than what might be called ‘LED purposes’, ‘including for archiving purposes in the public interest, scientific or

³⁰ TEU, Art. 6(1).

³¹ D. Bigo, G. Boulet, C. Bowden, S. Carrera, J. Jeandesboz and A. Scherrer, *Fighting Cyber Crime and Protecting Privacy in the Cloud* (European Parliament, October 2012), 36, https://pure.uva.nl/ws/files/1732778/148157_398380.pdf.

³² Declaration No. 21, [2016] OJ C 202, 7 June 2016, p. 345.

³³ GDPR, Art. 2(1).

³⁴ LED, Arts. 2(1) and 1(1).

historical research purposes or statistical purposes, unless the processing is carried out in an activity which falls outside the scope of Union law'.³⁵

Although the GDPR does not apply to law enforcement actors when discharging their core duties, law enforcement capacities are directly impacted by its growing influence on the private actors who are the source of much digital evidence. In particular it seems inevitable that full realisation of the data minimisation principle would mean less data available for criminal investigations.³⁶ A prime example, of key value in practice and carefully detailed by the European Commission in a dedicated Annex to its Impact Assessment accompanying the e-Evidence package, is the WHOIS directory service for domain names, part of which has (controversially) long remained publicly accessible.³⁷ With the GDPR being applied from May 2018 onward and the uncertainty surrounding the suitable legal basis under the Regulation for such public access, ICANN (Internet Corporation for Assigned Names and Numbers) has been grappling with how to ensure compliance without domain name registries having to move to closed systems,³⁸ causing an important investigatory starting point to dry up as a direct consequence of data protection enforcement.

The data minimisation principle also dovetails with the continued lack of an EU-level obligation on communications service providers to retain metadata for later use by law enforcement. The result is that investigations are hampered from the outset: typically, where an internet protocol (IP) address has been obtained from a service provider, it will be necessary to ask an internet access provider (or, if it keeps logs, a virtual private network (VPN) service provider) to determine who used defined IP addresses at specific times. Given the absence of an EU-level data retention regime in combination with a tightening of the data minimisation principle, the data may well be gone.³⁹

Of course, the reason for the continued lack of a unified data retention obligation at EU level is well-known: the CJEU's seminal case law from *Digital Rights Ireland* (2014)⁴⁰ and *Tele2* (2016),⁴¹ via *Privacy International*⁴² and *La Quadrature du Net* (both 2020),⁴³ up to the recent judgments in *GD*,⁴⁴ *VD and SR*⁴⁵ and *SpaceNet* (all 2022),⁴⁶ with little sign of the multifaceted

³⁵ LED, Art. 9(2), in conjunction with Recital 12. Emphasis added. We return to the precise contours of who or what might qualify as a 'competent authority' later.

³⁶ For a warning against the broader, potentially negative impacts of a strict application of the data minimisation principle on the practices of big data analysis across the board, see T. Z. Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 *Seton Hall Law Review* 1009–1012.

³⁷ European Commission, 'Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings' (Draft e-Evidence Regulation and draft Legal Representatives Directive), SWD(2018) 118 final, 17 April 2018 (COM e-Evidence IA), Annex 12.

³⁸ EDPB, 'The European Data Protection Board Endorsed the Statement of the WP29 on ICANN/WHOIS', 27 May 2018, https://edpb.europa.eu/news/news/2018/european-data-protection-board-endorsed-statement-wp29-icannwhois_en.

³⁹ COM e-Evidence IA, p. 23.

⁴⁰ Joined Cases C-203/12 and C-594/12, *Digital Rights Ireland and Seitlinger* [2014] ECLI:EU:C:2014:238.

⁴¹ Joined Cases C-203/15 and C-698-15, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others* [2016] ECLI:EU:C:2016:970 (*Tele2*).

⁴² Case C-623/17, *Privacy International* [2020] ECLI:EU:C:2020:790 (*Privacy International*).

⁴³ Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others* [2020] ECLI:EU:C:2020:791 (*La Quadrature du Net*).

⁴⁴ Case C-140/20, *GD v. Commissioner of An Garda Síochána and others* [2022] ECLI:EU:C:2022:258 (*GD*).

⁴⁵ Joined Cases C-339/20 and C-397/20, *VD and SR* [2022] ECLI:EU:C:2022:703 (*VD and SR*).

⁴⁶ Joined Cases C-793/19 and C-794/19, *Spacenet and Telekom Deutschland* [2022] ECLI:EU:C:2022:702 (*SpaceNet*).

line of jurisprudence stopping there.⁴⁷ The pertinence of the Court's position(s) on communications data retention to the relationship between data protection and direct cooperation is analysed in Section 3.3.2.

It suffices here to dwell briefly on the significance for direct cooperation of the ePrivacy Directive,⁴⁸ the legal instrument which 'particularises and complements' the standards set out in the GDPR with respect to the processing of personal data in the electronic communication sector, and is at the heart of the CJEU's data retention case law since *Tele2*. Although the precise relationship between the exclusory clause in Article 1(3) and the limitation clause in Article 15(1) provides its pressure point, the root of the data retention dispute is found in Articles 6 and 9 of the ePrivacy Directive. Article 6 establishes the rule that traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of the communication, for billing and payments, or for marketing (with subscriber or user consent). Article 9, meanwhile, provides that 'location data other than traffic data' may be processed only when it is made anonymous or this is done with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value-added service.⁴⁹

From 21 December 2020, the definition of the 'electronic communications services' (ECS) to which the above provisions apply was broadened by the introduction of the European Electronic Communications Code (EEC Code)⁵⁰ to include so-called number-independent interpersonal communications services (NI-ICS), such as OTT (over-the-top) services like VoIP (voice over internet protocol), messaging and web-based email services. According to McIntyre, the extension of the stronger confidentiality rules of Article 5 of the ePrivacy Directive to those services is likely to drive down voluntary disclosure to law enforcement and transfer greater pressure onto new schemes for formalised direct cooperation, particularly the EU e-Evidence package and the related EU-US agreement.⁵¹

Moreover, OTT services will be amongst the electronic communications services falling within the scope of the upcoming ePrivacy Regulation,⁵² which will eventually⁵³ replace the

⁴⁷ See further S. Eskens, 'The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-Depth Review of *La Quadrature du Net* and others and *Privacy International*' (2022) 8(1) *European Data Protection Law Review* 143–155.

⁴⁸ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications) (ePrivacy Directive), [2002] OJ L 201, 31 July 2002, pp. 37–47.

⁴⁹ The ePrivacy Directive, Art. 5 is also a very important protection as it binds member states to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications *and the related traffic data* by persons other than users, without the consent of the users concerned, except when legally authorised to do it through legislative measures. Emphasis added.

⁵⁰ Directive (EU) 2018/1972 of the European Parliament and the Council of 11 December 2018 establishing the European Electronic Communications Code (EEC Code), [2018] OJ L 321, 17 December 2018 pp. 36–214.

⁵¹ T. J. McIntyre, 'Voluntary Disclosure of Data to Law Enforcement: The Curious Case of US Internet Firms, Their Irish Subsidiaries and European Legal Standards', in F. Fabbrini, E. Celeste and J. Quinn (eds.), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Oxford: Hart, 2021), 20. Implementation of the EEC Code appears to be slow. See European Commission, 'EU Electronic Communications Code: Commission Refers 10 Member States to the Court of Justice of the EU', 6 April 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1975.

⁵² European Commission, Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), [2017] COM(2017) 10 final, 10 January 2017.

⁵³ At the time of writing, the latest available full text of the draft Regulation is the Council mandate from 10 February 2021. See Council of the European Union, Proposal for a Regulation of the European Parliament and

ePrivacy Directive. At the time of writing, the contents of the intensively lobbied new Regulation, and in particular whether it will overall maintain, raise or lower the levels of protection afforded by the old Directive (an instrument dating back to 2002), remain uncertain. For present purposes, it is worth highlighting the following provision in the Council's 2021 mandate regarding the Regulation's material scope: Article 2.2(a) provides that it will not apply to 'activities, which fall outside the scope of Union law, and in any event measures, processing activities and operations concerning national security and defence, regardless of who is carrying out those activities whether it is a public authority or a private operator acting at the request of a public authority'.⁵⁴ The wording of this provision as well as the timing of the mandate, four months on from the CJEU's decisions in *La Quadrature du Net* and *Privacy International*, leave little room for doubt that it was intended as a response to those rulings. In particular, the above provision squarely contradicts the Court's conclusion that the processing of personal data (including retention and transmission) by electronic communications service providers for the purpose of safeguarding national security falls within the scope of EU law – notwithstanding Article 4(2) of the Treaty on European Union (TEU).⁵⁵ For the European Data Protection Board (EDPB), this aspect of the Council mandate 'runs against the premise for a consistent EU data protection framework';⁵⁶ whilst Tzanou and Karyda observe that 'circumventing – or indeed abolishing – the CJEU's jurisprudence on data retention in the ePrivacy Regulation would also set a dangerous precedent for the Court's assessment of third country metadata retention laws and practices, such as the US, in light of *Schrems I* and *Schrems II*. Double standards in this regard risk rendering the CJEU's case law meaningless and cannot be accepted.'⁵⁷

3.2.2 The Law Enforcement Directive

Although Recital 10 of the LED makes reference to the aforementioned Declaration No. 21 to the Lisbon Treaty – which referred only to police and judicial cooperation – the scope of the Directive goes beyond such cooperation in order to include domestic law enforcement processing, that is, irrespective of whether data processing crosses national borders within the EU. For this reason alone, the LED constitutes a major upgrade on its predecessor, the 2008 Framework Decision, which applied only to cross-border processing.⁵⁸ In several other respects, however, as

of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (ePrivacy Regulation Council mandate), [2021] 2017/0003(COD), 10 February 2021, <https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf>.

⁵⁴ ePrivacy Regulation Council mandate, s. 42.

⁵⁵ *Privacy International*, para. 44. TEU, Art. 4(2) reads:

The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. *In particular, national security remains the sole responsibility of each Member State.* (Emphasis added)

⁵⁶ Adding that '[i]n the event of an exclusion, the EDPB stresses nevertheless that the GDPR applies'.

⁵⁷ M. Tzanou and S. Karyda, 'Privacy International and *Quadrature du Net*: One Step Forward Two Steps Back in the Data Retention Saga?' (2022) 28(1) *European Public Law* 152–153.

⁵⁸ Compare Art. 1(1) and Recital 7 of Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, [2008] OJ L 350, 30 December 2008, pp. 60–71.

is well-established in the literature,⁵⁹ compared to the GDPR, the LED ‘waters down’⁶⁰ the three cornerstones of EU data protection law: data processing principles, data subject rights and independent supervision.⁶¹

The vicissitudes of political compromise required in order to reach an outcome on the LED, combined with the heterogeneity of authorities, tasks and powers in the ‘law enforcement’ area across the member states, quickly prompted the academic literature to identify a host of reservations as to the approximation power of the instrument. The first of these is its personal and material scope.

As concerns personal scope, the question is in the first place which public authorities qualify as ‘competent authorities’ under the LED.⁶² Initial assessment of national implementations has suggested a wide divergence of approaches in the member states: for instance, closed lists of public authorities contrast with open-ended provisions which could include local authorities, assessed on a case-by-case basis, whilst some national provisions may well encompass foreign public authorities.⁶³ The application of the LED to cross-border cooperation between national financial intelligence units (FIUs) which are classed as administrative authorities in some member states and law enforcement authorities in others also warrants careful assessment.⁶⁴

Regarding material scope, the wording of Recital 12 has enabled several national legislators to attach their LED-implementing rules (in place of the GDPR) to data processing relating to minor offences, administrative offences or all types of offence – and thus far beyond ‘criminal offences’ strictly speaking.⁶⁵ In daily practice, and even where only public authorities are involved, it may prove difficult to cleanly settle which regime applies in certain scenarios: consider police officers (an LED ‘competent authority’) processing personal data for identification or verification purposes in the field of migration and border control (which are not ‘LED purposes’).⁶⁶

⁵⁹ J. Sajfert and T. Quintel, ‘Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities’, in M. Cole and F. Boehm (eds.), *GDPR Commentary* (Cheltenham: Edward Elgar, in press), <https://ssrn.com/abstract=3285873>. Castets-Renard presents the three main areas of weaknesses in the LED as (i) excessively supple directing principles, (ii) limited data subject rights and (iii) inadequacy of data controller obligations (translation author’s own). See C. Castets-Renard, ‘Directive 2016/680/UE et réforme des données personnelles en matière pénale: Le droit européen en quête de protection et cohérence’, in É. Debaets, A. Duranthon and M. Sztulman (eds.), *Les fichiers de police* (Bayonne: Institut Universitaire Varenne, 2019), 401–419, especially 404–416.

⁶⁰ P. De Hert and V. Papakonstantinou, ‘The New Police and Criminal Justice Data Protection Directive: A First Analysis’ (2016) 7(1) *New Journal of European Criminal Law* 18.

⁶¹ See further De Hert and Sajfert, ‘The Role of the Data Protection Supervisory Authorities’, 244–247.

⁶² The question of whether private entities may qualify as competent authorities under the LED is subject to a dedicated analysis in Section 3.3.1.2 *et seq.*

⁶³ See, e.g., P. Vogiatzoglou and S. Fantin, ‘National and Public Security within and beyond the Police Directive’, in A. Vedder, J. Schroers, C. Ducuing and P. Valcke (eds.), *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security* (Cambridge: Intersentia, 2019), 27–62, 48–57.

⁶⁴ F. Mouzakiti, ‘Cooperation between Financial Intelligence Units in the European Union: Stuck in the Middle between the General Data Protection Regulation and the Police Data Protection Directive’ (2020) 11(3) *New Journal of European Criminal Law* 351–374, 363–374; M. Brewczyńska, ‘Financial Intelligence Units: Reflections on the Applicable Data Protection Legal Framework’ (2021) 43 *Computer Law & Security Review*, 1–14, 11–13.

⁶⁵ Sajfert and Quintel, ‘Data Protection Directive (EU) 2016/680’, 3–4. See also, e.g., LED, Recital 13: ‘A criminal offence within the meaning of this Directive should be an autonomous concept of Union law as interpreted by the Court of Justice of the European Union.’ The Commission recently expressed the view that LED, Recital 13 ‘entails, among other things, that Member State law cannot determine the nature of an offence as being “criminal” for the sole purpose of applying the LED’. See European Commission, First Report on Application and Functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 (LED) (COM LED Report), [2022] COM(2022) 364 final, 25 July 2022, p. 11.

⁶⁶ T. Quintel, ‘Data Protection Rights for Third Country Nationals? Harmonization Prospects under EU Data Protection Reform’, PhD thesis, University of Luxembourg (2021).

Turning to data subject rights under the LED, from the point of view of both criminal investigators and the defence, it is perhaps the discrepancy between the ‘right to information’ enshrined in Article 14 of the GDPR and the ‘information to be made available or given to the data subject’ in Article 13 of the LED which most stands out. The latter provision includes two tiers of information: more general information⁶⁷ which is to be *made available* (hence: a static notice on a webpage will suffice) to the data subject, and

further information to enable the exercise of his or her rights: (a) the legal basis for the processing; (b) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period; (c) where applicable, the categories of recipients of the personal data, including in third countries or international organisations; (d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.⁶⁸

Whilst the level of prescriptiveness is low, this is a suite of information that the average criminal defence⁶⁹ would gladly seize upon in order to prepare its strategy. However, the LED permits member states to adopt legislative measures delaying, restricting or omitting the provision of the second tier of information to the data subject in order to:

- (a) avoid obstructing official or legal inquiries, investigations or procedures;
- (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- (c) protect public security;
- (d) protect national security;
- (e) protect the rights and freedoms of others.⁷⁰

The scope for restrictions is thus potentially very broad, but, importantly, even where member states choose to limit the information provided to data subjects under Article 13(3), the LED introduces a duty on member states to ensure that certain data subject rights, including that in Article 13(2), can be indirectly exercised by data protection authorities (DPAs).⁷¹

For the reasons evoked in this subsection, to mention only a few, the Commission’s first report on the evaluation and review of the LED, due on 6 May 2022,⁷² was keenly awaited. Following the implementation deadline of 6 May 2018, a total of nineteen member states had faced infringement proceedings for non-transposition; by July 2019, three member states faced

⁶⁷ Identity and contact details of the controller; contact details of the data protection officer, where applicable; intended purposes of the data processing; right to lodge a complaint with a supervisory authority and contact details of that authority; existence of the right to request from the controller access to and rectification or erasure of personal data; and restriction of processing of the personal data concerning the data subject (LED, Art. 13(1)(a)–(e)).

⁶⁸ LED, Art. 13(2).

⁶⁹ Without forgetting convicts, victims and (expert) witnesses, the focus here is primarily on investigator and target: the suspect, accused or defendant.

⁷⁰ To the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned; LED, Art. 13(3).

⁷¹ LED, Art. 17. Questioning whether indirect access fulfils the main purposes of the right of access, see further D. Dimitrova and P. De Hert, ‘The Right of Access under the Police Directive: Small Steps Forward’, in M. Medina, A. Mitrakas, K. Rannenberg, E. Schweighofer and N. Tsouroulas (eds.), *Privacy Technologies and Policy: 6th Annual Privacy Forum, APF 2018, Barcelona, Spain, June 13–14, 2018, Revised Selected Papers* (Cham: Springer, 2018), 111–130, especially 123–124.

⁷² LED, Art. 62.

actions⁷³ and in 2022 fresh proceedings for incomplete or inadequate implementation were launched against four member states.⁷⁴ The Commission report was eventually released in July 2022,⁷⁵ finding that whilst on the whole national laws ‘largely reflect the LED’s principles and core provisions’, a large number of outstanding issues remain, including both the delineation of the scope of the LED and the GDPR and data subject rights.⁷⁶

In those respects and more, the (first) report on the LED is, however, of limited value in that – unlike the customary style of an evaluation report – it does not provide a full breakdown (by provision in the Directive, by country and/or by regulatory option triggered) of the national implementations. This can admittedly be partly explained by the diversity of approaches taken at national level: whilst in several member states the LED has been implemented in the same legal act as the GDPR (and in many instances national laws transpose the LED by referring to the same or equivalent provision of the GDPR), a number of the LED’s provisions have also been transposed through new provisions in, for instance, general administrative law, administrative procedural law or criminal procedure. Furthermore, some member states have transposed a number of the LED’s provisions in sectoral legislation regulating the operation and powers of specific competent authorities (e.g. police law). ‘A variety of national legal acts’, the Commission concludes, ‘may therefore have to be considered when determining whether or not the LED has been correctly transposed in a particular Member State.’⁷⁷

Notwithstanding these brakes on comparability, it is regrettable that a more thorough overview has not been provided: for present purposes, little can be gleaned from the report’s general observations on the LED’s scope of application as enshrined in national implementing laws.⁷⁸ As concerns data subject rights, the Commission reports that all member states have chosen to make use of the possibility in Article 15(1) LED to restrict data subjects’ right of access – but stops short of providing an overview of those restrictions. ‘Most’ member states reportedly also provide for restrictions of information to be made available or given to the data subject under Article 13 (discussed earlier) and/or the right to rectification or erasure of personal data and restriction of processing in Article 16 LED. The report continues: ‘The national data protection acts transposing the LED often only follow the general language of the LED without further specifying the circumstances or the conditions in which the restrictions are to apply. In such cases, these circumstances and conditions have to be specified in sectoral legislation otherwise it would give

⁷³ T. Wahl, ‘Infringement Proceedings for Not Having Transposed EU Data Protection Directive’, *Eucrium*, 10 September 2019, eucrium.eu/news/infringement-proceedings-not-having-transposed-eu-data-protection-directive/. See, e.g., Case C-658/19, *European Commission v. Kingdom of Spain* [2021] ECLI:EU:C:2021:138. Spain was ordered to pay a lump sum of €15 million plus a daily penalty payment of €89,000 for each day from the day of the judgment onwards (provided the infringement still obtains) until it has put an end to the infringement.

⁷⁴ In April 2022: Finland and Sweden – both lack access to effective judicial remedy for data subjects (respectively, INFR(2022)4010 and INFR(2022)2022); Germany – there are gaps in the transposition of the LED in relation to the German Federal Police (INFR(2022)2019); Greece – the implementing (national) legislation is not in conformity with the EU legislation being implemented (the LED) on a number of points (INFR(2022)2021). In May 2022: Germany – several national laws fail to provide effective corrective powers at federal and *Länder* level (INFR(2022)2030).

⁷⁵ COM LED Report.

⁷⁶ Other priority areas, in the Commission’s view, are governance and powers of DPAs; remedies; time limits for storage and review of personal data; legal basis for processing, including special categories of personal data; automated decision-making; distinction between categories of data subjects; distinction between classes of personal data and verification of its quality; and logging. See COM LED Report, 9–16.

⁷⁷ COM LED Report, 9.

⁷⁸ ‘Some Member States consider that a number of administrative bodies (e.g. FIUs) carry out tasks falling under the LED’; ‘(a) few Member States have also provided a derogation for processing by certain types of competent authorities or certain types of data’; ‘some national transposing laws refer to purposes for processing personal data that are not listed in Article 1 LED (e.g. threats to public order or public safety)’. See COM LED Report, 11.

data controllers discretion in applying these restrictions.⁷⁹ The lack of detail on national implementations of, *inter alia*, the data subject rights provided by the LED not only is relevant to gauging the success of that Directive as a harmonisation measure but also makes it more difficult to discern the data protection basis upon which new direct cooperation tools such as the e-Evidence Regulation would operate.

The key data protection provision in the draft e-Evidence Regulation, corresponding to Article 13 of the LED, was undoubtedly Article 11 on ‘Confidentiality and user information’.⁸⁰ And whilst in principle nothing would appear to stop the e-Evidence reform bringing in tighter standards on notifying data subjects who have been targeted by a European Production Order (EPO) or a European Preservation Order, the potential ramifications for national levels of protection remain difficult to map without a clearer picture of implementation of the LED. We return to the contested incorporation of notification of data subjects in the e-Evidence package in Section 3.4.1.2, after exploring how EU data protection law deals with public–private cooperation on digital evidence in Section 3.3.

3.3 EU DATA PROTECTION AND PUBLIC–PRIVATE COOPERATION ON DIGITAL EVIDENCE

During the gestation period of the GDPR and the LED, efforts had been made by the European Parliament rapporteurs on both files to explicitly address the conundrum of public–private data processing arrangements which will inevitably engage both instruments. To this end, Jan Philipp Albrecht (GDPR rapporteur) had proposed to exclude from the scope of the Regulation data processing ‘by competent *public* authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties’, thereby opening the possibility that it could apply to non-public actors when processing personal data for one of those same purposes.⁸¹ Meanwhile, Dimitrios Droutsas (LED rapporteur) proposed the insertion of a new article into the Directive capable of encompassing private-to-public data flows (termed ‘access to data initially processed for purposes other than those referred to in Article 1(1)’).⁸²

Ultimately, in the final texts any binding provision on the data protection implications of public–private cooperation in law enforcement was conspicuously absent. This raises the question of which regime should apply to what aspects of interactions between public and private actors in the law enforcement space. In the ensuing sections, that question is explored using two essential pieces of the basic ‘grammar’ of EU data protection law: data controller and data processor.

The data controller is defined as ‘the natural or legal person, public authority, agency or other body’ (GDPR) or the ‘competent authority’ (LED) ‘which, alone or jointly with others, determines the purposes and means of the processing of personal data’.⁸³ The data processor, meanwhile, is defined identically in both instruments: “processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller’.⁸⁴

⁷⁹ COM LED Report, 15.

⁸⁰ G. Robinson, ‘The European Commission’s e-Evidence Proposal’ (2018) 4(3) *European Data Protection Law Review* 350.

⁸¹ LIBE Committee, Draft Report on GDPR Proposal, 17 December 2012, Amendment 80, p. 62 (emphasis added).

⁸² LIBE Committee, Draft Report on LED Proposal, 20 December 2012, new Art. 4a, Amendment 58, pp. 39–40.

⁸³ GDPR, Art. 4(7); LED, Art. 3(8).

⁸⁴ GDPR, Art. 4(8); LED, Art. 3(9).

Three starting points can be distinguished in the context of direct cooperation on digital evidence: public–private cooperation under the LED only; instances of public–private cooperation which engage both the LED and the GDPR; and the matter of the informal direct cooperation in light of the GDPR. The following subsections analyse each of these scenarios in turn through the lens of the two above-cited pieces of EU data protection law grammar: data controller and data processor.

3.3.1 *Public–Private Cooperation under the LED*

3.3.1.1 ‘Delegation’: Public LED Controller–Private LED Processor

The most straightforward scenario of public–private cooperation involving digital evidence is that of controller and processor under the LED. Typical examples might be a forensic lab carrying out expert analysis of evidence in criminal proceedings on assignment of a court, prosecutor or the police,⁸⁵ and a cloud service provider contracted to store a court’s digital archives.⁸⁶ Such arrangements are characterised by a lack of agency for the processor, who acts ‘on behalf of’ the controller, in principle following without deviation the controller’s instructions.

The onus is on member states to ensure that LED controllers use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the LED, and to ensure the protection of the rights of the data subject – although the weight of the latter criterion is reduced by the requirement in Article 22(3)(b) of the LED that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The controller is thus in sole charge of whether to inform the data subject of the processing of their data, in accordance with the national implementation of the LED data subject rights regime, discussed in Section 3.2.2.

Member states shall also provide for the processing by a processor to be governed by a contract or other legal act under Union or member state law that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.⁸⁷

This scenario (*public LED controller–private LED processor*) applies most cleanly to situations where data processing takes place solely on the basis of a contract containing crystal-clear instructions. To return to the example of a forensics lab, usually the very first contact such

⁸⁵ T. Gottschalk, ‘The Data-Laundromat? Public-Private-Partnerships and Publicly Available Data in the Area of Law Enforcement’ (2020) 6(1) *European Data Protection Law* 34.

⁸⁶ N. Purtova, ‘Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public-Private Partnerships’ (2018) 8(1) *International Data Privacy Law* 64.

⁸⁷ LED, Art. 22(3) further provides:

That contract or other legal act shall stipulate, in particular, that the processor: (a) acts only on instructions from the controller; (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (c) assists the controller by any appropriate means to ensure compliance with the provisions on the data subject’s rights; (d) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless Union or Member State law requires storage of the personal data; (e) makes available to the controller all information necessary to demonstrate compliance with this Article; (f) complies with the conditions referred to in paragraphs 2 and 3 for engaging another processor.

a lab will have with the material to be analysed will be governed by the contract with the controller. The very first processing of the relevant data therefore also takes place as a direct consequence of the contractual arrangement – as should, if all goes to plan, all subsequent processing until the end of the arrangement.

However, should such a processor at any stage determine the purposes and the means of processing, that processing can no longer be deemed to be performed ‘on behalf of’ the controller. As a result, the processor infringes the LED and is considered to be a controller in respect of that processing.⁸⁸ The precise contours of ‘on behalf of’ will vary depending on the circumstances, and it is no doubt unreasonable to demand that all technical minutiae of outsourced expert analysis be set out in advance in a contract.

In many cases, the reason a law enforcement authority requires the services of external data processors in the first place is that the public authorities are unable to do something themselves – for instance, ‘brute force’ a seized digital device using a proprietary technique that investigators are unable to acquire for (regular) in-house use. In such situations, the controller’s instructions ‘may still leave a certain degree of discretion about how to best serve the controller’s interests, allowing the processor to choose the most suitable technical and organisational means’,⁸⁹ but any independent determination by the processor of the purposes or the means of the processing risks triggering controllership. A case-by-case analysis remains necessary, confirms the EDPB, ‘in order to ascertain the degree of influence each entity effectively has in determining the purposes and means of the processing’.⁹⁰

In order to avoid risking a violation of the LED by a processor exceeding its remit, as clear a contract as possible is thus advisable. But contracts are not the only means by which a controller–processor relationship may be established under the LED: any ‘legal act under Union or Member State law that is binding on the processor with regard to the controller’⁹¹ may potentially suffice, thus going beyond consensual agreements to cover the imposition of LED processor status.

The *public LED controller–private LED processor* scenario becomes more complex, above all for the private entity and the data subject, in situations where an LED processor must combine this contractual role under the LED with processing the same data under the GDPR for other purposes (typically, commercial ones). Interactions between the GDPR and the LED in this kind of situation are analysed in detail in Section 3.3.2, after a second scenario more cleanly confined to the LED alone is addressed in Section 3.3.1.2.

3.3.1.2 ‘Private Competent Authorities’: Public LED Controller–Private LED Controller

Section 3.3.1.1 showed that if an LED processor crosses a certain threshold of agency, it may de facto become an LED controller ‘by accident’. But the Directive also opens the space for a private entity to become a data controller under the LED by design – when it is appointed as a private ‘competent authority’. As noted earlier, in Article 3(7) of the LED one finds a twofold

⁸⁸ As provided by LED, Art. 22(5), mirroring GDPR, Art. 28(10).

⁸⁹ EDPB, ‘Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. Version 2.0’, 7 July 2021, para. 80, p. 26. As the Commission recently noted, whilst LED, Art. 51 sets out the EDPB’s tasks in relation to processing within the scope of the Directive, ‘[m]any of the EDPB’s guidelines on the GDPR are also relevant for the LED to the extent that they rely on common concepts or technologies. Such guidelines include those on the concept of data controller and processor’. See COM LED Report, 24.

⁹⁰ EDPB, ‘Guidelines 07/20’, para. 82, p. 27.

⁹¹ See LED, Art. 22(3) and the stipulations therein as to the minimum contents of the contract or other legal act. Comparing data processor status to delegation, see also EDPB, ‘Guidelines 07/20’, para. 80, p. 26.

definition of ‘competent authority’: any public authority competent for Article 1(1) purposes or ‘any other body or entity entrusted by Member State law to exercise public authority and public powers’ for those same purposes.⁹²

In its July 2022 report on the ‘application and functioning’ of the LED, the Commission shared its view that ‘competent authorities’ as defined by the LED are

either organs of the State or private bodies, on which the law confers special powers beyond those which result from the normal rules applicable in relations between individuals and/or by the possibility of exercising the power of coercion. These authorities are competent authorities under the LED when (even if only sporadically and/or in isolated cases) they process data for the purpose of preventing, investigating, detecting or prosecuting criminal offences or of executing criminal penalties (including safeguarding against and preventing threats to public security).⁹³

Regarding the national implementations, the Commission reported: ‘Most of the Member States’ laws comprehensively cover any competent authority processing of data for LED purposes. By contrast, some Member States have chosen to exhaustively enumerate the competent authorities under the LED in their national legislation. A few Member States have also provided a derogation for processing by certain types of competent authorities or certain types of data.’

Regrettably, no further information is shared on whether, which and how member states have used the possibility to allow for ‘private competent authorities’ in national laws. However, the emerging literature would seem to confirm that at least some member states have taken up this option. For example, through a combined reading of national legislation and DPA guidance in six member states, Vogiatzoglou and Fantin have placed the Republic of Ireland, Italy and France (together with ex-member state the United Kingdom) into that camp.⁹⁴

For all of the EU-27 which have done likewise, it will be instructive to make out the precise contours in national law of the phrase ‘entrusted by Member State law to exercise public authority and public powers’ for LED purposes. It was noted in Section 3.2.2 how Recital 12 of the Directive has led to a broadening of the scope of *public* competent authorities in certain implementations. In relation to *private* competent authorities, a thorough comparative view would take in the following aspects for each jurisdiction: how *private* competent authorities may be designated ‘by Member State law’ (primary or secondary legislation, law or decree, closed list or case-by-case designations?); exactly what public authority and/or powers may be entrusted to them as data controllers;⁹⁵ and the identity and the tasks of private entities currently thus designated in each member state.

Whilst the wording ‘entrusted’ by law to exercise public authority and public powers (and a fortiori, for instance, the wording ‘authorised’ in the Irish act implementing the LED⁹⁶) might suggest a limitation to private entities which willingly take on the role of private competent authority (e.g. a company joining a public–private partnership (PPP) to combat

⁹² Only the public limb of this definition had been included in the Commission proposal from 2012 (Art. 3(14)), with the second limb – added during negotiations – opening up the potential for application of the LED to private actors.

⁹³ COM LED Report, 10.

⁹⁴ Vogiatzoglou and Fantin, ‘National and Public Security’, 51–57.

⁹⁵ Purtova remarks, furthermore: ‘It appears that it is possible for such a private party to be seen as a competent authority for the purposes of the Directive even when the national law does not formally recognize it as a law enforcement authority, but grants public authority and public powers for the law enforcement purposes in Article 1(1) (LED)’; Purtova, ‘Between the GDPR and the Police Directive’, 66. All the same, and as she also notes (at 65–66), Art. 3(8) LED states that ‘where the purposes and means of (processing by a competent authority) are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law’. This provision mirrors Art. 4(7) of the GDPR.

⁹⁶ Data Protection Act 2018, s. 69(1)(b).

cybercrime),⁹⁷ it seems likely that a private entity may be made an LED competent authority by law without its having sought such a role: for instance, ‘critical infrastructures’ identified in the framework of EU legislation.⁹⁸ Yet other entities may be difficult to categorise as either public or private: for instance, a state-owned public transport company put in charge, by national law, of handling ticket offences.

For the fruits of a private competent authority’s data processing to be used by a public competent authority, and inherently so for digital evidence, some form of data transfer between a private competent authority and a public competent authority will usually be required. In such circumstances, ‘where two or more controllers jointly determine the purposes and means of processing’, member states are bound by Article 21 LED to provide for them to be joint controllers. They shall, moreover,

in a transparent manner, determine their respective responsibilities for compliance with (the LED), in particular as regards the exercise of the rights of the data subject and their respective duties to provide the information referred to in Article 13,⁹⁹ by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement shall designate the contact point for data subjects. Member States may designate which of the joint controllers can act as a single contact point for data subjects to exercise their rights.

Dividing up responsibilities between joint LED controllers will be more straightforward when the data in question is processed exclusively for LED purposes: for instance, a privately run prison under contract with the national prison service to process inmates’ personal data. Such a private competent authority will still have to juggle its role as an LED controller for prisoner data with parallel responsibilities under the GDPR in relation to other personal data – for instance, staff data for HR purposes¹⁰⁰ – but a clear demarcation between legal regimes is in place, laying the foundation for the assignment of respective roles by contract or other legal act.

Matters become less clear-cut whenever the *same data* is processed by a private processor (tackled in Section 3.3.1.1) or a private joint controller (as just discussed) under the LED for its purposes as well as under the GDPR for other purposes. An example that could fit either scenario – to the extent that personal data is in play – is a private entity performing blockchain analytics both for commercial market analysis and to assist cryptocurrency-related investigations.¹⁰¹

⁹⁷ Purtova, ‘Between the GDPR and the Police Directive’, 52.

⁹⁸ See Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, [2008] OJ L 245, 23 December 2008, pp. 75–82. Given the ‘body or entity’ wording in the LED, the private competent authority would be the ‘European critical infrastructure’ (ECI) itself, rather than its owner/operator or Security Liaison Officer. This example is also put forward by Vogliatzoglou and Fantin, ‘National and Public Security’, 50.

⁹⁹ Discussed in Section 3.2.2.

¹⁰⁰ Similarly to public authorities processing data for different purposes, including EU institutions, bodies, offices and agencies (IBOAs) such as the European Public Prosecutor’s Office (EPPO) with two different data protection regimes for operational and administrative personal data. See, e.g., V. Franssen and M. Corhay, ‘Interpretation of the EPPO Regulation in View of EPPO’s Supervision by the EDPS’, *European Data Protection Supervisor*, 12 April 2021, https://edps.europa.eu/data-protection/our-work/publications/reports/interpretation-epo-regulation-view-eppos-supervision_en.

¹⁰¹ For example, Chainalysis. See, e.g., M. Fröwis, T. Gottschalk, B. Haslhofer, C. Rückert and P. Pesch, ‘Safeguarding the Evidential Value of Forensic Cryptocurrency Investigations’ (2020) 33 *Forensic Science International: Digital Investigation*, 1–14. ‘[W]here forensic analyses are outsourced and conducted by (private) third parties . . . , the GDPR can remain applicable.’

Taking private LED *processors* first, Recital 11 restates that ‘the application of (the GDPR) remains unaffected for the processing of personal data outside the scope of this Directive’. Of itself, this does not provide a conclusive answer to the ‘two hats’ conundrum identified in the literature: a private actor processing personal data as an LED processor on behalf of an LED controller is bound to confidentiality under that legal instrument,¹⁰² but must *also* comply with data subject rights under the GDPR – in this case Articles 13 and 14 GDPR. Without a clear selection of legal regime in law,¹⁰³ the dual application of both regimes is thus liable to give rise to dual, conflicting obligations.¹⁰⁴

Turning to the second scenario, private competent authorities acting as *joint controllers* under the LED will often simultaneously handle the same personal data under the GDPR, for other purposes. This situation mirrors that of a public competent authority (e.g. police, prosecutor or judge) which must apply either the LED for processing pertaining to their core functions or the GDPR for any other purpose. It also immediately throws up a host of questions as to how several provisions of the LED could be applied by private controllers, whether regarding key data processing principles¹⁰⁵ or data subject rights – especially where comparable duties exist in the GDPR in relation to the very same data.¹⁰⁶ In any case, as seen earlier, a private competent authority must be entrusted with public authority and public powers by member state law – providing an opportunity to ensure much-needed clarity on respective responsibilities from the start of joint processing operations.

At the EU level, the Commission’s direct cooperation mechanism as envisaged in the initial e-Evidence package would appear to neatly fit the LED joint controllership provisions in several core respects: there is processing of data for LED purposes, with the exercise of public authority and powers entrusted to a private entity and the means of processing at least co-determined by that private entity – a fortiori where production orders must be assessed for manifest violation of fundamental rights and/or abuse.¹⁰⁷

Whilst both the EU Council and the European Parliament subsequently excised that particular test from their starting positions for trilogues, instances wherein the LED applies instead of the GDPR cannot be discounted so long as the e-Evidence Regulation limits itself to mentioning that the two instruments apply as an *acquis*. As Corhay has opined, ‘[o]ne can regret

¹⁰² LED, Art. 22(3)(b).

¹⁰³ Or a clear restriction of the scope of application of the GDPR under Art. 23; given this chapter’s focus on digital evidence in criminal matters, such a restriction would be based on Art. 23(1)(d) GDPR.

¹⁰⁴ Purtova, ‘Between the GDPR and the Police Directive’, 65–66. The point has also been raised within the Commission Expert Group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, citing the example of a law enforcement authority engaging a private company as a processor in order to decrypt a hard disk for investigation purposes. For some members,

(s)uch situations raised difficulties in application of different legal regimes to the same data sets, in particular as regards data subject rights. The Commission suggested that national laws could lay down the rules on joint controllership and responsibility for the personal data in such databases, as well as the rules on the point of contact for data subjects (conversely Art. 26(1) GDPR).

See Commission Expert Group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Minutes of the Fifteenth Meeting, 20 February 2018, <https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=3656&fromExpertGroups=true>.

¹⁰⁵ For instance, the distinction between different categories of data subject as required by LED, Art. 6 or the duty in LED, Art. 7(1) to distinguish personal data based on facts from personal data based on personal assessment.

¹⁰⁶ Compare, for instance, LED, Art. 16 (on the right to rectification or erasure of personal data and restriction of processing) with GDPR, Arts. 16–20.

¹⁰⁷ Decried by Mitsilegas as a de facto ‘privatisation of mutual trust’. See V. Mitsilegas, ‘The Privatisation of Mutual Trust in Europe’s Area of Criminal Justice: The Case of e-Evidence’ (2018) 25(3) *Maastricht Journal of European and Comparative Law* 263.

that, so far, the EU institutions have missed the opportunity to adopt a position on some important questions such as the instrument – the GDPR or the LED – that must apply when public authorities access data stored by private actors’.¹⁰⁸ The risks attached to overlapping legal regimes are further unpacked in Section 3.3.2.

3.3.2 Public–Private Cooperation, the LED and the GDPR: Public LED Controller–Private GDPR Controller

Having reiterated the space created in Article 3(7) LED for the appointment of non-public bodies or entities as competent authorities under this Directive, Recital 11 LED begins to address the attendant risk of overlapping EU data protection regimes as follows:

Where such a body or entity processes personal data for purposes other than for the purposes of this Directive, Regulation (EU) 2016/679 applies. Regulation (EU) 2016/679 therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. For example, for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law.

Reflecting the fact that the two instruments together formed a package, the first sentence mirrors the carve-out in Article 2(2)(d) of the GDPR, in its final form without the Albrecht amendment mentioned in Section 3.3.¹⁰⁹ The first clause in the second sentence also merely restates the *lex generalis* baseline: where a body or entity collects personal data for ‘other purposes’ (i.e. non-LED purposes), the GDPR should apply.¹¹⁰ So far, so consistent.

The second clause of the second sentence then ostensibly refers to Article 6(1)(c) of the GDPR, establishing a legal basis for data processing where ‘necessary for compliance with a legal obligation to which the controller is subject’. Yet this is not the same as asserting that *only* the GDPR may apply to such further processing – for instance, where digital evidence is transferred to a public LED data controller. In other words, on a literal reading the eventuality that a private entity may act simultaneously as GDPR controller and LED joint controller in relation to (at least) a transfer of data between cooperating entities is not discounted. On this view, the transfer of digital evidence between private actor and public authority would no longer fall between the cracks of the EU data protection legal framework, as the consensus in doctrine had it before the 2016 reforms,¹¹¹ but be subject to a mild form of hyperregulation: the *lex specialis*

¹⁰⁸ M. Corhay, ‘Private Life, Personal Data Protection and the Role of Service Providers’ (2021) 6(1) *European Papers* 471.

¹⁰⁹ ‘This Regulation does not apply to the processing of personal data: ... (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’

¹¹⁰ ‘Should’ apply since the breadth of this assertion (‘other purposes’) is already open to question on the grounds that the GDPR does not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, pursuant to Art. 2(2)(a) of the GDPR. The Regulation, although of *general* application, was never designed to cover processing for *all* possible purposes. See M.-E. Ancel, ‘D’une diversité à l’autre: A propos de la “marge de manœuvre” laissée par le règlement général sur la protection des données aux États membres de l’Union européenne’ (2019) 2019(3) *Revue critique de droit international privé* 647.

¹¹¹ G. Boulet and P. De Hert, ‘Cooperation between the Private Sector and Law Enforcement Agencies: An Area in between Legal Regulations’, in H. Aden (ed.), *Police Cooperation in the European Union under the Treaty of Lisbon: Opportunities and Limitations* (Baden-Baden: Nomos, 2015), 245–258.

(carrying lower standards of protection) can apply on top of the *lex generalis* (carrying higher standards of protection).

Furthermore, the lack of any ascription of data controllership in Recital 11 also generates uncertainty: when a private actor, in compliance with a legal obligation upon it, transfers digital evidence to investigators, where does controllership arise? Joint controllership is a possibility under the LED, but even where this does not obtain (for instance, where the private actor is not on a closed list of LED competent authorities determined in national law) and the GDPR alone applies, is joint controllership under the GDPR conceivable?

It might seem counterintuitive to consider that an entity which is constrained by a legal obligation can be labelled a *controller*, but this is the position taken by Purtova, one of (very) few scholars to have traced in detail what she calls the ‘maze’ of information sharing in PPPs in light of both the GDPR and the LED.¹¹² Whilst there will be many scenarios in which the GDPR controller’s decisional agency is reduced to virtually zero (for instance, where a prosecutor orders production of specific subscriber data behind a defined IP address),¹¹³ in Purtova’s view, even when it is under a legal obligation to ‘further process’ data, a certain degree of control always remains with the initial controller under the GDPR: ‘the private party should assess if the processing is necessary and proportionate to satisfy the legal obligation at hand, how much and which data is necessary and sufficient, whether providing for anonymous data would suffice or identifiable data is necessary, etc.’¹¹⁴ This in turn connects to an ongoing debate within EU data protection law and policy, well away from the world of cross-border criminal investigations (and rather too distant to cover in depth here), surrounding a fragmented conceptualisation of data controllership seemingly advocated by the CJEU in *Fashion ID*.¹¹⁵

For present purposes, it suffices to illustrate one important related unclarity emerging from jurisprudence closer to home: the aforementioned twin judgments in *Privacy International* and *La Quadrature du Net*. As seen in Section 3.2.1, it was the extension of *effet utile* reasoning (previously employed by the Court in relation to national data retention legislation measures for the combating of crime) to data retention for national security purposes, thus pulling the latter within the scope of EU law – and the inevitable thorough proportionality assessment – which has garnered most attention¹¹⁶ and triggered diverse responses in the member states¹¹⁷ as well as a confrontational ePrivacy Regulation mandate from the Council.

In *Privacy International* and *La Quadrature du Net*, the Court’s assignment of legal regimes turns on personal scope: wherever data processing obligations are imposed on providers of ECS, whether to safeguard national security or combat crime, the ePrivacy Directive applies to that

¹¹² Purtova, ‘Between the GDPR and the Police Directive’, 52.

¹¹³ As Purtova indeed identifies. See *ibid.*, 64.

¹¹⁴ *Ibid.*

¹¹⁵ Case C-40/17, *Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629. See M. Zalnieriute and G. Churches, ‘When a “Like” Is Not a “Like”: A New Fragmented Approach to Data Controllership’ (2020) 83(4) *Modern Law Review* 861–876; M. Finck, ‘Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law’ (2021) 11(4) *International Data Privacy Law* 333–347.

¹¹⁶ Pointing out a viable alternative interpretation of the relevant provisions in the ePrivacy Directive. See Iain Cameron, ‘Metadata Retention and National Security: *Privacy International* and *La Quadrature du Net*’ (2021) 58 *Common Market Law Review* 1458. For criticism of the reasoning used by the Court to distinguish away its earlier decision in PNR (Joined Cases C-317/04 and C-318/04, *Parliament v. Council and Commission* [2006] ECLI:EU:C:2006:346). See Tzanou and Karyda, ‘One Step Forward Two Steps Back’, 128–129.

¹¹⁷ S. Vallée and G. Genevoix, ‘A Securitarian Solange: France Has Launched a Cluster Bomb on the EU’s Legal and Political Order’, *Verfassungsblog*, 25 April 2021, <https://verfassungsblog.de/a-securitarian-solange/>; Cécile de Tervangne, ‘L’illégalité nuancée de la surveillance numérique: La réponse des juridictions belge et française à l’arrêt *La Quadrature du Net* de la Cour de Justice de l’Union Européenne’ (2022) 129 *Revue trimestrielle des droits de l’homme* 3–27.

processing.¹¹⁸ By contrast, where member states ‘directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of [ECS], the protection of the data of the persons concerned is covered not by the ePrivacy Directive, but by national law only, subject to the application of the [LED]’.¹¹⁹ Viewed through this chapter’s prism of public–private cooperation on digital evidence, at least three questions are left on the table by the Court’s *clivage* in *Privacy International* and *La Quadrature du Net*.

The first question is linked to what the Court does *not* state: that where ECS providers process data for the safeguarding of national security or the combating of crime pursuant to a legal obligation, *only* the ePrivacy Directive applies. Indeed, as the ePrivacy Directive is much less detailed than the GDPR, ECS providers will need to rely on the latter instrument wherever the former instrument has not ‘supplemented and specified’ it¹²⁰ – for instance, to ascertain obligations with regard to data processing principles and data subject rights. At the same time, application of the LED is not excluded by the Court.

Second, does the ECS provider act as a data processor or a (joint) controller, and under which instrument(s)? The Court does not provide concrete guidance in this regard, beyond a construal of Articles 23(1)(d) and (h) GDPR to observe that ‘the processing of personal data carried out by individuals for those same purposes falls within the scope of that Regulation’.¹²¹ There is an echo here of the Court’s *effet utile* reasoning with regard to the scope of Article 15(1) ePrivacy Directive: in essence, if there is a limitation clause, that which may be limited by such a clause must fall within the scope of the instrument. Yet it is the use of the word ‘individuals’, which does not appear in the cited provisions of the GDPR, which puzzles. Although the cited passage of the judgments is doubtless obiter, might the Court be offering, *sotto voce*, space now to accommodate ‘private competent authorities’ under the LED and/or room to manoeuvre in future for a fragmented notion of data controllership?

The answer matters since the bifurcated edifice of the EU data protection *acquis* is fundamentally challenged by data processing which shifts between ‘public’ and ‘private’ realms, whether in isolated instances or in the course of more stable partnership-like arrangements, inherently engaging both GDPR and LED. Most evidently, the purpose limitation principle enshrined in Article 5(1)(b)¹²² GDPR risks being effectively emptied should data handled by private service providers ‘slip’ from the ambit of the GDPR to the prosecutor, judge, police or other competent authority, operating (for core purposes) under the LED.¹²³

The average EU citizen, unversed in the highly legalistic nature of the data protection discussion, is well entitled to wonder: how can the second processing purpose *not* be ‘incompatible’ with the first?¹²⁴ Furthermore, once data is transferred to the competent authority side, the

¹¹⁸ *Privacy International*, para. 46; *La Quadrature du Net*, para. 101.

¹¹⁹ *Privacy International*, para. 48; *La Quadrature du Net*, para. 103.

¹²⁰ *Privacy International*, para. 47; *La Quadrature du Net*, para. 102.

¹²¹ *Privacy International*, para. 46; *La Quadrature du Net*, para. 102.

¹²² Personal data shall be: ... collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’).

¹²³ LED, Art. 4(1)(b) includes the purpose limitation principle, but this is limited to the collection of data under the LED. In most private-to-public scenarios, data will initially have been collected under the GDPR.

¹²⁴ See further Article 29 Working Party, Opinion 03/2013 on Purpose Limitation, 2 April 2013, 23–27, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf; and C. Jasserand, ‘Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation’ (2018) 2 *European Data Protection Law Review* 152–167. Along similar lines, see Advocate General Szpunar’s observation, in

supplier LED rules kick in: in particular, unlike the Regulation,¹²⁵ the Directive does not contain the concept of ‘further processing’. Subsequent processing by the same or a different competent authority is allowed for other LED purposes, if this is provided for by law, necessary and proportionate.¹²⁶

The obvious (and perhaps only) reply is that the incompatibility of such secondary use is exceptionally justified by the needs of law enforcement to obtain the personal data in order to perform their tasks. Investigative needs, simply put, trump purpose limitation. To borrow the conceptual lens of De Hert and Gutwirth, the ‘channelling’ function of data protection law is here much more present than its ‘blocking’ function.¹²⁷ Yet when the free movement of data – the ‘forgotten twin’ objective of EU data protection law¹²⁸ – wins out and once purpose limitation is forgone in the reuse of privately gathered data for the public purposes of law enforcement – what then remains of that channelling function? If the immediate rejoinder is ‘data subject rights and independent supervision’, effective fulfilment of the latter can only be hampered by such levels of indeterminacy as regards the applicable legal regime(s).

Returning to the questions left on the table post-*Privacy International* and *La Quadrature du Net*, the third question pertains to the space in between the two poles distinguished by the Court and marks the way to the final part of Section 3.3. In distinguishing the obligation to retain data and the relevant provisions on accessing that data (which *do* fall within the scope of the ePrivacy Directive for the purposes of the Court’s fundamental rights check) from the ‘direct implementation’ of data processing measures by public authorities (which escapes that check, and is subject to national law *only*), the judgments remain silent on voluntary cooperation. Now, it seems logical to surmise that an absence of clarity in the data protection parameters of formal public–private cooperation on digital evidence has contributed to (or even arguably sustained¹²⁹) the growth of informal ‘voluntary’ cooperation between ECS and law enforcement both domestically and transnationally. Section 3.3.3 examines this last scenario in more detail.

Before proceeding to voluntary cooperation, however, it is worth underlining that the studied case law concerns ‘only’ ePrivacy Directive *regulates* – which already covers a lot of digital evidence, but far from every source. It is also indelibly linked to that legal instrument, in the sense that the priorities and vision of the EU legislator calibrated at the turn of the millennium, as expressed in the Directive’s articles and recitals, drives much of the Court’s argumentation – in terms of normative load-balancing as well as interpretation of black-letter law. In months and

para. 131 of his Opinion in *Penalty Points*, that ‘private companies might be tempted to exploit personal data for commercial purposes, that is to say, for purposes that are incompatible with the purpose of the processing, which is to increase road safety’. See Opinion of Advocate General Szpunar in Case C-439/19 *B v. Latvijas Republikas Saeima (Penalty Points)*, [2020] ECLI:EU:C:2020:1054.

¹²⁵ See, e.g., GDPR, Recital 50, also discussed in Section 3.3.3.

¹²⁶ LED, Art. 4(2). See further Commission Expert Group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, Minutes of the Third Meeting, 7 November 2016, <https://ec.europa.eu/transparency/expert-groups-register/core/api/front/expertGroupAdditionalInfo/27802/download>. Of course, in contrast to the GDPR, in the law enforcement context the consent of the data subject cannot be a ground for data processing. See, e.g., LED, Recital 35.

¹²⁷ For the cited authors, the blocking function of data protection law renders the individual opaque to public power and corresponds to *privacy*, in contradistinction to its channelling function, which accepts that the data subject is rendered transparent to public power, in return for the constraining and reciprocal transparency of use of that power: appropriately circumscribed data processing principles, meaningful data subject rights and effective independent supervision. See P. De Hert and S. Gutwirth, ‘Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of Power’, in E. Claes, A. Duff and S. Gutwirth (eds.), *Privacy and the Criminal Law* (Antwerp: Intersentia, 2006), 61–104.

¹²⁸ TFEU, Art. 16; GDPR, Art. 1(1).

¹²⁹ A. Aguinaldo and P. De Hert, ‘European Law Enforcement and US Data Companies: A Decade of Cooperation Free from Law’ (2020) 6(26) *Brussels Privacy Hub Working Paper* 1–16, www.Brusselsprivacyhub.eu/Publications/Wp626.

years to come, it will be imperative to track the extent to which the incoming ePrivacy Regulation reflects and respects the Court's positioning so far, and influences it thereafter.¹³⁰

3.3.3 Informal Direct Cooperation and the GDPR: Public LED Controller–Private GDPR Controller

In the here and now, the consensus seems to have it that most cooperation between internet service providers (ISPs) and law enforcement is taking place on an 'informal' or voluntary basis – voluntary in the sense that the service provider's local law (i.e. where the service provider is headquartered or represented) does not explicitly recognise an 'order' or request from foreign law enforcement as legally binding. Local law often also positively prohibits compliance with a foreign-origin request – as exemplified in a transatlantic setting by the so-called *Microsoft Ireland* litigation,¹³¹ and within the EU by the *Skype* case.¹³² In such cases, any cooperation afforded will be voluntary – but it will also represent in principle a (conscious) violation of local law and risk attracting the relevant sanctions.

In most EU jurisdictions, as in *Skype* (at the time, headquartered in Luxembourg), domestic implementations of the ePrivacy Directive prohibit the voluntary direct divulgence of user data to foreign investigators by ECS including – since the EEC reform of late 2020 – many OTT services. Where no such bar is in place, the question arises of the compatibility of informal direct cooperation with data protection law – first and foremost, the GDPR. In this chapter, the cooperation of EU-based service providers with investigators in third countries (such as the United States) is set aside in order to focus on cooperation within the EU, with a view to complementing certain national chapters on EU member states in this volume.

McIntyre is one of few commentators to have closely examined the legal position of ISPs involved in informal cooperation with foreign investigators – in his case, providers based in Ireland – in terms of its compatibility with the purpose limitation principle and the legal bases for such processing which may be available in the GDPR. McIntyre determines that, save in exceptional cases such as where a provider detects fraud in relation to its own service and reports it to law enforcement, much voluntary cooperation with foreign investigators will not fulfil the five criteria set down in Article 6(4) GDPR.¹³³ As those criteria are non-exhaustive, a discrete analysis will be required in each instance of voluntary cooperation.

¹³⁰ See Also X. Tracol, 'The Joined cases of *Dwyer*, *SpacNet* and *VD and SR* before the European Court of Justice: The Judgments of the Grand Chamber about Data Retention Continue Falling on Deaf Ears in Member States' (2023) 48 *Computer Law & Security Review* 105773, 1–14.

¹³¹ See D. M. Sullivan, 'Brief of EU Data Protection and Privacy Scholars as Amici Curiae in Support of Respondent in *United States of America v. Microsoft Corporation*', 18 January 2018, www.supremecourt.gov/DocketPDF/17/17-2/28272/20180118141249281_17-2%20BSAC%20Brief.pdf. The author was one of twenty-one signatories of the amicus brief.

¹³² Belgian Supreme Court, 19 February 2019, P.17.1229.N.

¹³³ In the absence of both the data subject's consent and a Union or member state law pursuant to Article 23(1) GDPR, the controller 'shall take into account, inter alia:

any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

the possible consequences of the intended further processing for data subjects;

the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Should compatibility between one purpose and the next not obtain, the lawfulness of the processing can only be preserved by either the consent of the data subject (a non-starter in the criminal investigation context) or ‘a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard’ the objectives (including the combating of crime) referred to in Article 23(1) GDPR, and also meets the cumulative requirements set down in Article 23(2). Each national system will then fall to be assessed against those requirements. In the case of Ireland, McIntyre concludes that the blanket disapplication of the purpose limitation principle in national law will generally leave voluntary disclosure in breach of that principle;¹³⁴ from a broader EU perspective, it was noted in Section 3.2.2 that the Commission’s recent report on the implementation of the LED has shed little light on the situation across the member states.

Turning to the matter of a suitable GDPR legal basis for the voluntary disclosure of data to foreign investigators, McIntyre notes the consensus¹³⁵ shared by the European Data Protection Supervisor (EDPS), the EDPB and in the academic literature that the only possible grounds are protection of the vital interests of a natural person¹³⁶ – connoting emergency, and as such inherently of limited application – or the legitimate interests of the data controller or a third party.¹³⁷ Recital 50 to the GDPR states that ‘[i]ndicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller’. But given its tenor (*‘indicating possible criminal acts’*), the provision sits much more neatly with own-initiative notification of the relevant competent authority by the controller than with requests for digital evidence addressed by such an authority to service providers.¹³⁸

Lastly, to the extent that legitimate interests can be established as a ground for processing in the context of informal cooperation on digital evidence, that ground in any case dissolves where it is overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.¹³⁹ This in turn requires an individualised assessment of the need for disclosure and the impact on the data subject.¹⁴⁰ For McIntyre, the upshot is that service provider policy or practice of blanket voluntary disclosure to law enforcement on the basis of a request are per se unlawful.¹⁴¹ For the purposes of this chapter, and not for the first time, close similarities between the implications of such an individualised assessment and the Commission’s 2018 vision for the European Production and Preservation Orders, and in particular their vetting by service providers for manifest violations of Charter rights, hove into view.

¹³⁴ McIntyre, ‘Voluntary Disclosure of Data to Law Enforcement’, 10–11.

¹³⁵ Ibid., 11 and the sources cited there, in footnotes 48 and 49.

¹³⁶ GDPR, Art. 6(1)(d).

¹³⁷ GDPR, Art. 6(1)(f).

¹³⁸ McIntyre, ‘Voluntary Disclosure of Data to Law Enforcement’, 12.

¹³⁹ Ibid.

¹⁴⁰ GDPR, Recital 47 and McIntyre, ‘Voluntary Disclosure of Data to Law Enforcement’, 13, citing Article 29 Working Party, ‘Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC’, [2014] 844/14/EN.

¹⁴¹ McIntyre, ‘Voluntary Disclosure of Data to Law Enforcement’, 13.

3.4 DIGITAL EVIDENCE REFORMS IN THE TWO EUROPE¹⁴²3.4.1 *The EU e-Evidence Package*

At first glance, the dual-instrument e-evidence package¹⁴³ presented by the European Commission in April 2018 does not seem to have all that much to do with data protection. There is no reference to ‘data protection’ in the binding articles of the draft e-Evidence Regulation, and the GDPR and the LED are mentioned obliquely in just one article (Article 17), which provides that ‘effective remedies’ under national law against EPOs will be available at the eventual criminal proceedings in the issuing state ‘without prejudice’ to data protection remedies under the *acquis*. As for the accompanying draft LRD, there is no reference to ‘data protection’ in its main text.

Of the draft Regulation’s sixty-six (non-binding) recitals, ‘data protection’, the GDPR or the LED are mentioned in seven. One is a boilerplate closing reference to prior consultation of the European Data Protection Supervisor (EDPS),¹⁴⁴ and another evokes requirements on national authorities and service providers to put in place suitable technical measures for the public–private direct cooperation regime, including data security.¹⁴⁵ Two further recitals make a general reference to the existing EU data protection *acquis* in the context of justifying stricter controls in the mechanism on access to certain categories of data (‘transactional data’ and content data) than to others (‘access data’ and subscriber data),¹⁴⁶ and briefly mention service providers’ liability arising from ‘good faith’ compliance with data orders.¹⁴⁷ As for the preamble to the LRD, a mere two recitals feature the terms.¹⁴⁸

The dearth of references to data protection in the legislative package can be partly explained by the two instruments’ legal bases, respectively judicial cooperation and the internal market – although it does invite inquiry as to where policy priorities lie.¹⁴⁹ In the accompanying Impact Assessment,¹⁵⁰ one begins to see the multifaceted role played by data protection (and privacy) in the e-Evidence debate. It is possible to discern three main features.

First, as the proposal covers only electronic evidence which is already in existence (for instance, call records or message contents backed up by a tech company), the strengthening of data protection rules is recognised in the Commission’s Impact Assessment as a threat to the very availability of digital evidence for investigations. In particular, as noted in section 2.1 of the Impact Assessment, a comprehensive embedding of the principle of data minimisation would reduce the amount and types of data entering the ‘pipe’. From an enforcement perspective, the

¹⁴² The expression is borrowed from P. De Hert, G. González Fuster and B.-J. Koops, ‘Fighting Cybercrime in the Two Europes: The Added Value of the EU Framework Decision in the Council of Europe Convention’ (2006) 77(3) *Revue internationale de droit pénal* 503–524.

¹⁴³ For a more comprehensive analysis, see Chapter 7 in this volume.

¹⁴⁴ Draft e-Evidence Regulation, Recital 66.

¹⁴⁵ *Ibid.*, Recital 57.

¹⁴⁶ *Ibid.*, Recital 23.

¹⁴⁷ *Ibid.*, Recital 46. The remaining two Recitals are reminders – for the co-legislators (Recital 2) and for the member states implementing the Regulation (Recital 56) – of the status of data protection as a fundamental right.

¹⁴⁸ One (Recital 24) similarly provides for consultation of the EDPS, and the other (Recital 6) draws a parallel between the envisaged appointment of legal representatives for the ‘receipt of, compliance with and enforcement of’ (this language from Recital 7) orders to produce or preserve electronic evidence and the existing requirement to establish a legal representative for data protection matters under the GDPR.

¹⁴⁹ For criticism of the choice of legal basis for the draft Regulation, *inter alia* from a territorial sovereignty perspective, see M. Böse, ‘An Assessment of the Commission’s Proposals on Electronic Evidence’, *European Parliament*, 21 September 2018, 35–37, [www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2018\)604989](http://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2018)604989).

¹⁵⁰ COM e-Evidence IA.

logic of data minimisation is compounded by the continued absence of an EU-level obligation on communications service providers to retain traffic and location data.

Second, there is fragmentation: increasingly divergent data protection and privacy rules (and their application at national level) are represented in the Commission's Impact Assessment as a block in the pipeline of direct cooperation. This concern mirrors the single biggest driver of the proposal per se: the discrepancies and lack of clarity surrounding the legality of cross-border direct cooperation have already generated levels of legal uncertainty, which is detrimental to law enforcement as well as service providers, and action at the EU level is required lest the national laws of more member states shift to a generalised extraterritorial use of enforcement jurisdiction.¹⁵¹

The third and last main role played by data protection in the Commission's e-Evidence package reflects the global scene on which criminal investigations increasingly play out. Indeed, although they are EU law measures, the mooted European Production and Preservation Orders are inescapably extraterritorial by design: by proposing to retire data storage location as determiner of jurisdiction, the EU legislator is only too aware of the risks, first, of generating conflicts of law and, second, of triggering the adoption abroad of (further) reciprocal measures targeting European service providers.¹⁵² On a broader and longer view, there is arguably also the potential for uncoordinated extensions of the 'sword' of law enforcement into the cloud to fuel a worldwide shift to data localisation and a future of fractured 'data sovereignties'.¹⁵³

Given these friction risks, the EU legislator has included the safety net of a review procedure in case of conflicting obligations under third country law,¹⁵⁴ whilst in parallel the co-legislators also espouse the goal of including EU data protection norms in their external action, partly in order to ensure their fulfilment within the Union.¹⁵⁵ Even in the absence of any international agreement, the EU legislator aims to deliver in the e-Evidence reform 'a measure that contains strong safeguards and explicit references to the conditions and safeguards already inherent in the EU [data protection] *acquis*, thus serving as a model for foreign legislation'.¹⁵⁶

The following subsections reflect on the likely impact of the e-Evidence reform on effective data protection within the EU, addressing successively the models put forward by the European Commission, the EU Council and the European Parliament, before the discussion narrows, in Section 3.4.1.2, to focus on the 'gateway right' of 'information to the data subject', that is, notification of the target of an investigation. A final subsection, Section 3.4.1.3, then offers a first reaction to the final text of the e-Evidence Regulation, which emerged just as this chapter was being finalised.

¹⁵¹ Compare Böse, who argues that the proposed mechanism will not fully overcome the current fragmentation of divergent cooperation regimes in the Member States' criminal justice systems. See Böse, 'An Assessment of the Commission's Proposals', 43–45.

¹⁵² In particular, business organisations responding to the open consultation on the e-Evidence reform highlighted the need for a 'full assessment of the risks arising from reciprocal action of non-EU countries'; COM e-Evidence IA, p. 126. In this vein, see further in the same document pp. 96, 105, 124, 127 and 171.

¹⁵³ Ligeti and Robinson, 'Sword, Shield and Cloud', 70.

¹⁵⁴ See Draft e-Evidence Regulation, Arts. 15–16; and Chapter 7 in this volume.

¹⁵⁵ See, e.g., this press release from the Council of the European Union, 'Council Gives Mandate to Commission to Negotiate International Agreements on e-Evidence in Criminal Matters', 6 June 2019, www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/, and Part III ('Safeguards') of the e-evidence negotiating directive accessible therefrom. See also, more recently, Directorate-General for Justice and Consumers, 'EU–U.S. Announcement on the Resumption of Negotiations on an EU–U.S. Agreement to Facilitate Access to Electronic Evidence in Criminal Investigations', European Commission, 2 March 2023, https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en.

¹⁵⁶ Draft e-Evidence Regulation (see note 5), p. 10.

3.4.1.1 Data Protection and the European Production Order

3.4.1.1.1 EUROPEAN COMMISSION: DE FACTO JOINT CONTROLLERSHIP. In the Commission model, European Production (and Preservation) Orders are addressed to the legal representative or potentially any establishment of the service provider in the Union.¹⁵⁷ In Section 3.3.1.2, it was argued that the ‘manifest violation/abuse’ control operated by service providers¹⁵⁸ could imply joint controllership status under the GDPR – or potentially even the LED – for those private entities.

The lack of decisive ascription of controllership in the proposals was strongly criticised by the EDPB, with the Board expressing concern that the definition of ‘service provider’ to mean ‘any natural or legal person that provides one or more of the following categories of services’¹⁵⁹ in conjunction with a broad definition of ‘offering services’¹⁶⁰ could cover both controllers and processors (for instance, processors storing data for controllers) in the sense of the GDPR.¹⁶¹ This matters above all since, by its nature, a processor acts on instructions given by the controller; it is the responsibility of the latter to ensure that the rights of data subjects are respected. In concrete terms, should a *processor* (say, a storage service in Member State B) receive one of the new orders to produce or preserve digital evidence instead of a *controller* (say, the legal representative based at headquarters in Member State A), the former would not receive access requests from data subjects and will not be in a position to answer such requests unless expressly asked to do so by the latter. Meanwhile, where it is the processor who receives an order to produce or preserve digital evidence, the controller receiving access requests from the data subject may simply not have (all) the sought information. The result in practice, fears the Board, could be a de facto dilution or even circumvention of data subject rights (provided that such rights have not already been limited in Union or member state law in full compliance with Article 23 GDPR).¹⁶²

Both EDPB and EDPS have, more broadly, called for clarification of the roles to be played by legal representatives under the LRD and legal representatives under the GDPR, given the ‘important differences in terms of role, liability and relationship with the other establishments of the service provider in one case and controller or processor in the other’. They recommend that two different legal representatives should be designated, each with clear distinct functions according to the relevant instrument: e-Evidence or data protection.¹⁶³

3.4.1.1.2 EU COUNCIL: DELEGATION BACKED BY SANCTIONS. The first inroads into the Commission’s direct cooperation model appeared in December 2018 with inclusion in the Council’s general approach of a new Article 7a providing for notification of the competent authority of the putative enforcing state to take place simultaneously with the submission of orders to service providers. However, such notification is limited to (i) EPOs only, concerning (ii) content data only, where (iii) the issuing authority has reasonable grounds to believe that the person whose data is sought is not residing on its own territory and (iv) entails submission to the enforcing authority of the EPOC only (the Certificate also received by service providers), rather

¹⁵⁷ Ibid., Arts. 7(2)–(4).

¹⁵⁸ Ibid., Arts. 9(5), 14(4)(f) and 14(5)(e).

¹⁵⁹ Ibid., Art. 2(3).

¹⁶⁰ Ibid., Art. 2(4).

¹⁶¹ EDPB, ‘Opinion 23/2018 on Commission Proposals on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (Art. 70.1.b)’ (EDPB e-Evidence opinion), adopted 26 September 2018, pp. 9–10, https://edpb.europa.eu/sites/default/files/files/file1/eevidence_opinion_final_en.pdf.

¹⁶² Ibid., p. 10.

¹⁶³ Ibid., p. 11. The EDPS adds a third distinct legal representative: that appointed under the future ePrivacy Regulation; EDPS e-Evidence Opinion, pp. 16–17.

than the Order itself – or both.¹⁶⁴ The automatic notification of the enforcing state as envisaged by the Council is further limited by the fact that it does not have a suspensive effect on the obligations of service providers,¹⁶⁵ meaning firstly that the ten-day window for production is unaltered and assessment by the notified authority must proceed swiftly.¹⁶⁶

In its general approach, the Council thus largely maintains the Commission's positioning of service providers, but attempts to balance its own key priorities of national sovereignty and efficiency.¹⁶⁷ From a data protection perspective, as seen earlier in Section 3.3.1, that role resembles much more the 'delegation' which is characteristic of data processors: an instruction is carried out with very little, if any, scope for decisional agency. Crucially, however, in this arrangement failure to perform the duty delegated would result not in (mere) data protection and/or contractual liability but in pecuniary sanctions under the e-Evidence Regulation, as determined by the 'enforcing authority'.¹⁶⁸

3.4.1.1.3 EUROPEAN PARLIAMENT: AN EXPRESS EIO FOR DATA. Draft amendments to the Commission proposals released by the European Parliament's rapporteur in October 2019 insisted on a 'meaningful notification' of the rebaptised 'executing' – as opposed to 'enforcing' – authority. Notification, in the rapporteur's view, can be 'meaningful' only if it includes the right to refuse to recognise data orders – and this in relation to all types of data – on the basis of grounds for non-recognition or non-execution set out in a new Article 10a.¹⁶⁹ Those grounds are copied from the corresponding provisions in Article 11 EIO Directive, reflecting a general objective of refashioning the proposal into something of an 'express EIO for data', complete with a return to the familiar grounds for non-recognition or non-execution: optional for dual criminality; mandatory where a data order would be incompatible with a member state's obligations in accordance with Article 6 TEU and the Charter.

Reverting to the more familiar EIO dynamic also has consequences in terms of data protection. And whilst (echoing the EDPB and the EDPS) the Parliament proposed to narrow the personal scope of the Regulation to GDPR data controllers,¹⁷⁰ this is not the same as determining which legal regime is to apply to which part(s) of the cooperation chain: namely, when data travels from the service provider to the executing authority, and then onward to the issuing authority.

¹⁶⁴ Council of the European Union, Document 10206/19 (Council e-Evidence general approach), 11 June 2019, Art. 7a. Notwithstanding agreement on the general approach, reservations were entered by no fewer than nineteen member states on several component parts of the reworked mechanism; see Council e-Evidence general approach, p. 34.

¹⁶⁵ Council e-Evidence general approach, Art. 7a(4).

¹⁶⁶ The notified authority's room for pushback is also minimal: it may inform the issuing authority of 'circumstances' related to immunities or privileges granted under its law, to 'rules on determination and limitation of criminal liability relating to freedom of press and freedom of expression in other media' or to the potential impact on fundamental interests such as national security and defence, but there is no power to object and the tenor of the new provision clearly puts the emphasis on production where at all possible.

¹⁶⁷ As in the priorities of the majority: a group of five member states have made a reservation on this deletion, advocating, among other things, for the inclusion of a fundamental-rights clause in the provisions on conditions for issuing an EPOC(-PR), notification of the enforcing state and limitations on the use of data obtained; Council, Document 10206/19, p. 43.

¹⁶⁸ Draft e-Evidence Regulation, Arts. 13 and 14.

¹⁶⁹ European Parliament, Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on European Production Orders for Electronic Evidence in Criminal Matters (Sippel Report), 24 October 2019, pp. 96–99.

¹⁷⁰ Sippel Report, Amendment 87, expressly binding the definition of 'service provider' to the role of data controller under the GDPR.

The EIO Directive itself until very recently provided, in its Article 20, that member states were to ensure, when implementing that instrument, that personal data may be processed only in accordance with the 2008 Framework Decision and the principles of the Council of Europe's 'Convention 108'.¹⁷¹ Even reading in the LED in place of the reference to its predecessor¹⁷² was not sufficient to remedy a mismatch between the material scope of the LED (police and criminal justice) and other types of proceedings for which an EIO can be issued, which extend beyond criminal proceedings to include, for instance, punitive administrative proceedings.¹⁷³

Although its July 2021 report on the implementation of the EIO Directive made no mention at all of data protection,¹⁷⁴ the Commission had already acknowledged this potential for confusion in a proposal to amend the EIO Directive¹⁷⁵ – a recommendation initially made in a Communication which had assessed the need, in the interests of consistency, for steps to align a wide range of Third Pillar instruments with the LED.¹⁷⁶ The chosen solution was to delete Article 20 EIO Directive, effective as of March 2022, via amending Directive 2022/228.¹⁷⁷ The result, that amending Directive states in a recital, is that the processing of personal data under the EIO Directive for the purposes set out in Article 82 TFEU *should* comply with the LED – 'where that latter Directive applies' – whereas when personal data is processed under the EIO Directive in relation to formally non-criminal¹⁷⁸ proceedings as mentioned in Articles 4(b), (c) and (d) EIO Directive, where the LED does not apply, the GDPR will.¹⁷⁹

Member states had until 14 March 2023 to bring into force the laws, regulations and administrative provisions necessary to comply with this reform,¹⁸⁰ but it remains to be seen how far consistency and effective data protection (the twin goals of the reform)¹⁸¹ can be improved by the soft, qualified language included in the preamble. It will be important to monitor in future whether those member states which had chosen to apply the weaker LED rules

¹⁷¹ Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Convention 108), ETS No. 108, 28 January 1981. See further Section 3.4.2.

¹⁷² As required by LED, Art. 59.

¹⁷³ See EIO Directive, Art. 4(b)–(d).

¹⁷⁴ European Commission, *Report from the Commission to the European Parliament and the Council on the Implementation of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 Regarding the European Investigation Order in Criminal Matters*, [2021] COM(2021) 409 final, 20 July 2021.

¹⁷⁵ European Commission, *Proposal for a Directive of the European Parliament and of the Council Amending Directive 2014/41/EU, as Regards Its Alignment with EU Rules on the Protection of Personal Data*, [2021] COM(2021) 21 final, 20 January 2021, p. 4.

¹⁷⁶ See, European Commission, *Communication to the Parliament and Council on the Way Forward on Aligning the Former Third Pillar Acquis with Data Protection Rules*, [2020] COM/2020/262 final, 24 June 2020, pp. 10–11. LED, Art. 62(6) called upon the Commission to review other legal Acts adopted by the Union which regulate processing by competent authorities for LED purposes with a view to aligning those Acts with the LED.

¹⁷⁷ European Commission, *Directive (EU) 2022/228 of the European Parliament and of the Council of 16 February 2022 Amending Directive 2014/41/EU, as Regards Its Alignment with Union Rules on the Protection of Personal Data*, [2022] OJ L 39/1-3, 21 February 2022, Art. 1.

¹⁷⁸ According to the seminal *Engel* jurisprudence from the European Court of Human Rights (ECtHR) (*Engel and Others v. The Netherlands*, Appl. No. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72, 8 June 1976; adopted by the CJEU in Case C-489/10, *Bonda*, [2012] ECLI:EU:C:2012:319, para. 37), an offence bearing the 'administrative' label in national law may nonetheless satisfy the ECtHR's (autonomous) interpretation of a criminal charge for the purposes of applying Art. 6 ECHR, depending on the nature of the (so-called punitive administrative) offence and the severity of the penalty. In its judgment in *Penalty Points*, the CJEU applied the *Engel / Bonda* jurisprudence in determining the applicability of Art. 10 GDPR ('Processing of personal data relating to *criminal convictions and offences*') to a system of public disclosure of penalty points deducted for road traffic offences; Case C-439/19, *Latvijas Republikas Saeima (Penalty Points)*, [2021] ECLI:EU:C:2021:504, paras. 80–94.

¹⁷⁹ Directive 2022/228, Recital 2.

¹⁸⁰ Ibid., Art. 2(1).

¹⁸¹ Ibid., Recital 2.

to administrative offences (including in purely domestic cases) now consider themselves obliged to revise national rules in order to bring EIOs issued (inherently, cross-border) in relation to punitive administrative proceedings under the higher standards of the GDPR.

Comparably, and to bring the discussion back to the e-Evidence reform, it will also be important to assess the risk of member states construing the category of ‘all criminal offences’ so broadly as to cover administrative offences, thereby expanding the scope of the EPO.¹⁸² Especially for data subjects and service providers, but also for investigators, legal clarity and consistency seem certain to prove a key challenge in this regard in years to come.

3.4.1.2 The Gateway Right: Confidentiality and Information to the Data Subject

In a delicate balancing act, Article 11 of the Commission’s draft Regulation provides that the addressee of an EPOC or an EPOC-PR must ensure the confidentiality of the order (and of the data produced or preserved) but shall only refrain from informing the person whose data is being sought (in compliance with Article 23 GDPR) where this is requested by the issuing authority. Where the service provider has not already informed the data subject that their data has been subject to an EPOC or an EPOC-PR, it falls to the issuing authority to inform the target thereof once there is no longer a risk of obstructing the relevant criminal proceedings (in accordance with Article 13 LED). Once (if) apprised of the situation, the person whose data has been obtained via an EPO (whether a suspect or accused person or not; hence, whether in criminal or non-criminal proceedings) has the right to effective remedies under the EU data protection *acquis* and under national law before the court in the issuing state.¹⁸³

The co-legislators’ points of departure on Article 11 saw them at loggerheads: the Council’s agreed position would ensure secrecy by default, with the issuing authority in virtually full control of whether to inform the target,¹⁸⁴ whilst the Parliament’s rapporteur has proposed to make notification by the addressee (rather than the issuing authority) the rule, with any exception requiring a court order.¹⁸⁵ Meanwhile, some commentators suggested that ‘[t]he practical exercise of the right of data subjects to be informed could be enabled, for instance, through the involvement of trusted third parties (e.g. national data protection authorities)’.¹⁸⁶ Such a set-up is vulnerable to the charge of raising more questions than it solves, not least in terms of workability and resources. Moreover, the main principled argument against involving DPAs in such a way – that to do so would radically alter their role in national criminal justice systems – stands to reason. At the same time, it is submitted, it is also surely worth reflecting on whether such a mechanism would be (much) less radical than the ‘new dimension in mutual recognition’¹⁸⁷ entailing a relegation of the public hitherto-executing authority to a residual enforcement role, substituted in the base direct cooperation scenario with a private entity.

¹⁸² Under the Commission proposal, EPOs to produce subscriber data or access data may be issued for ‘all criminal offences’. See Draft e-Evidence Regulation, Art. 5(3).

¹⁸³ Ibid., Art. 17. Importantly, immunities and privileges in respect of transactional or content data obtained by virtue of an EPO granted under the law of the member state of the addressee (the service provider) are to apply in criminal proceedings in the issuing state.

¹⁸⁴ Council e-Evidence general approach, 38.

¹⁸⁵ Sippel Report, 99–101.

¹⁸⁶ S. Carrera and M. Stefan, ‘Access to Electronic Data for Criminal Investigations Purposes in the EU’ (2020) 1 *Liberty and Security in Europe* 66.

¹⁸⁷ COM e-Evidence IA, p. 37.

In any case, especially in light of the difficulties of preparing a criminal defence across borders in a likely unfamiliar jurisdiction, and a fortiori should the fundamental rights check on data orders by service providers be cursory or even removed (as proposed by the Council),¹⁸⁸ notification of data subjects functions as a gateway right in order for further protections or defence rights to be invoked.¹⁸⁹ As such, it was certain that once the outcome of the lengthy trilogues eventually surfaced in the form of a compromise text, many data protection and criminal defence lawyers would make a beeline for the settlement arrived at in this specific respect.

In early 2023, just as this chapter was being completed, that compromise text was released,¹⁹⁰ before July 2023 saw the Regulation published in the Official Journal.¹⁹¹ Although a full overview of its broader potential data protection ramifications is for future research efforts, Section 3.4.1.3 offers a first glimpse of the final e-Evidence Regulation – beginning where this subsection ends: with the notification of data subjects.

3.4.1.3 January 2023: Agreement on e-Evidence

In terms of confidentiality and information to the data subject, the final version of Article 11 – now renumbered Article 13 – is most in keeping with the EU Council’s late 2018 position, with a degree of compromise between co-legislators subtly visible in the structuring and contents of the provision. Thus, as a rule the issuing authority shall inform the person whose data is being sought without undue delay;¹⁹² there is no longer any mention of addressees or service providers informing data subjects.¹⁹³ However, an issuing authority may delay, restrict or omit informing the person whose data is being sought, to the extent that and for as long as the conditions in Article 13(3) LED are met. Reasons for doing so must be indicated in the case file, and a short justification must be added in the Certificate.¹⁹⁴

The settlement reached on notification of the data subject sits within an overall cooperation mechanism which blends elements from each of the co-legislators’ visions. In terms of the ‘directness’ of that cooperation, Article 8 plays a crucial role. Reflecting the European Parliament’s priorities, that provision establishes a system of notification with suspensive effect (except in emergency cases) of the competent authority of the ‘enforcing state’.¹⁹⁵ However, its weight is subject to a double limitation. On the one hand, reflecting the Commission’s initial wish to streamline access to less sensitive data categories, it applies only to content data and traffic data ‘except when the latter is requested for the sole purpose of identifying the user’. On the other hand, reflecting the Council’s stance, notification does not kick in at all – even to those

¹⁸⁸ As discussed in Section 3.4.1.1.2.

¹⁸⁹ Carrera and Stefan, ‘Access to Electronic Data’, 53–57.

¹⁹⁰ Council of the European Union press release, ‘Electronic Evidence: Council Confirms Agreement with the European Parliament on New Rules to Improve Cross-Border Access to e-Evidence’, 25 January 2023, www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/.

¹⁹¹ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (e-Evidence Regulation), [2023] OJ L191, 28 July 2023.

¹⁹² e-Evidence Regulation, Art. 13(1). See also Recital 67.

¹⁹³ Those entities are bound to ensure the *confidentiality, secrecy and integrity* of the EPOC or the EPOC-PR and of the data produced or preserved. See e-Evidence Regulation, Art. 13(4), emphasis added.

¹⁹⁴ e-Evidence Regulation, Art. 13(2).

¹⁹⁵ *Ibid.*, Art. 8(4). Accordingly, grounds for refusal for EPOs (immunities and privileges, freedom of the press and freedom of expression, manifest breach of ‘a relevant fundamental right’, *ne bis in idem* and double criminality) are set out in Art. 12.

more sensitive data categories – ‘if, at the time of issuing the Order, there are reasonable grounds to believe that (a) the offence has been committed, is being committed or is likely to be committed in the issuing State; and (b) the person whose data are sought resides in the issuing State’.¹⁹⁶ Given the subjective nature of this pivot between indirect and direct cooperation, to be operated by issuing authorities, in future it will be essential that the transparency standards in the e-Evidence Regulation are upheld: in particular, overall numbers of EPOCs issued¹⁹⁷ against the number of notifications sent to the enforcing authorities.¹⁹⁸

High levels of discretion for the issuing authority are also visible as regards the interface of the EU data protection *acquis* and the e-Evidence mechanism. The final compromise text specifies that EPOs ‘shall be addressed to service providers, acting as data *controllers*, in accordance with [the GDPR]’, or – exceptionally – to data *processors* where ‘the controller cannot be identified despite reasonable efforts on the part of the issuing authority, or addressing the controller might be detrimental to the investigation’.¹⁹⁹ The bar is set at ‘reasonable efforts’, whilst a recital explains:

distinguishing between the roles of controller and processor with regard to a particular set of data requires not only specialised knowledge of the legal context, but could also require interpretation of often very complex contractual frameworks providing in a specific case for allocation to various service providers of different tasks and roles with regard to a particular set of data. Where service providers process data on behalf of a natural person, it may be difficult in some cases to determine who the controller is, even where there is only one service provider involved.²⁰⁰

The same provision also explains that a controller, even when identified, may not be a suitable addressee in the eyes of the issuing authority where that controller is a suspect or accused or convicted person in the case concerned ‘or there are indications that the controller could be acting in the interest of the person that is the subject of the investigation’.²⁰¹ Once more, the bar is set rather low, with the slightest risk of jeopardising an investigation warranting the directing of orders to a data processor.

Where processors receive orders, the rule is that they shall inform the controller – not of the fact of receiving an order but ‘about the production of the data’.²⁰² Whilst this wording is fuzzy (does it mean that the controller is apprised that data has already been produced, that data is about to be produced,²⁰³ or merely that an order has been received?), it seems likely that the question is largely moot, given that the issuing authority may request on open grounds that the service provider refrain from informing the controller ‘for as long as [is] necessary and proportionate, in order not to obstruct the relevant criminal proceedings’.²⁰⁴ In light of this discretion afforded to the issuing authority, it is regrettable to find no specific requirement in the final Regulation to record and report reasons for the choice to opt for direct cooperation with a data

¹⁹⁶ e-Evidence Regulation, Art. 8(2).

¹⁹⁷ *Ibid.*, Art. 28(2)(a).

¹⁹⁸ *Ibid.*, Art. 28(2)(d).

¹⁹⁹ *Ibid.*, Art. 5(6), emphasis added.

²⁰⁰ *Ibid.*, Recital 42.

²⁰¹ *Ibid.*

²⁰² *Ibid.*, Art. 5(7).

²⁰³ Compare the wording of the notification to be made in principle to the data subject, i.e. the person ‘whose data *are being requested*’. See e-Evidence Regulation, Art. 13(1), emphasis added.

²⁰⁴ Similarly to the mechanism for notification of the data subject, ‘the issuing authority shall indicate in the case file the reasons for the delay in informing the controller. A short justification shall also be added in the EPOC.’ See e-Evidence Regulation, Art. 5(7).

processor rather than a data controller, where the controller is identifiable, or indeed the reasonable efforts made to identify it before ordering data from a processor.

Lastly, it is worth underlining that whilst the final e-Evidence Regulation does engage with the data protection status (controller or processor) of addressees of an EPO and regulate interactions between those parties as well as the data subject, it makes no mention of the data protection regime(s) which may be applicable to the *transfer* of data to the relevant authorities.²⁰⁵ It thus leaves unaffected the analysis made heretofore in this chapter, particularly in Sections 3.2 and 3.3.

3.4.2 *The Second Additional Protocol to the Budapest Convention*

3.4.2.1 Direct Cooperation under the Protocol, Signature and Ratification

As the e-Evidence reform inched its way towards finalisation throughout 2022, the EU was also preparing its reception of the Council of Europe's kindred spirit: the 2nd Protocol.²⁰⁶ In April 2022, the EU Council adopted a decision authorising member states to sign the 2nd Protocol.²⁰⁷ Signature and subsequently ratification would constitute the next milestones on the long path taken by the reform through the Cybercrime Convention Committee (T-CY) drafting process, which began in September 2017, before in June 2019 the Commission received a mandate from the member states to begin negotiating the protocol directly with the Council of Europe.²⁰⁸

In the final agreed mechanism, direct cooperation consists of requests for domain name registration information (Article 6) and disclosure of subscriber information (Article 7).²⁰⁹ For the former, there is no scope for parties to enter reservations. For the latter, in contrast, a host of options exists. Parties may:

- reserve the right not to apply Article 7 (Article 7.9.a);
- reserve the right not to apply Article 7 to 'certain types of access numbers' (Article 7.9.b);
- make (upon signature or ratification) the following declaration: 'The order under Article 7, paragraph 1, must be issued by, or under the supervision of, a prosecutor or other judicial authority, or otherwise be issued under independent supervision' (Article 7.2.b);
- notify (upon signature or ratification or at any other time) the Secretary General of the Council of Europe that, when an order for subscriber information is issued to a service provider in its territory, it requires, in every case or in identified circumstances, simultaneous notification of the order, the supplemental information and a summary of the facts related to the investigation of proceeding (Article 7.5.a) to a single designated authority.²¹⁰

²⁰⁵ See, e.g., e-Evidence Regulation, Arts. 10(2)–(3).

²⁰⁶ See also Chapter 8, this volume.

²⁰⁷ Council Decision (EU) 2022/722 of 5 April 2022 authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (Council 2nd Protocol signature decision), [2022] OJ L 134, 11 May 2022, pp. 15–20.

²⁰⁸ European Commission press release, 'Security Union: Commission Receives Mandate to Start Negotiating International Rules for Obtaining Electronic Evidence', 6 June 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2891. See P. De Hert and A. Aguinaldo, 'A Leading Role for the EU in Drafting Criminal Law Powers? Use of the Council of Europe for Policy Laundering' (2019) 10(2) *New Journal of European Criminal Law* 99–106.

²⁰⁹ Pursuant to Art. 5(7), the direct cooperation provisions in the 2nd Protocol do not restrict cooperation between parties, or between parties and service providers or other entities, through other applicable agreements, arrangements, practices or domestic law. On this level, therefore, the EU e-Evidence reform is unaffected.

²¹⁰ See Art. 7.5.b–f for further details of options and procedures on notification.

Whilst the overlap in core tensions with the EU e-Evidence reform addressed in some detail earlier is self-evident, it is important to highlight fundamental differences between the EU's and the Council of Europe's initiatives – both related to the matter of whether and to what extent the latter are to be taken as legally binding.

First, at the 'lower' level of direct public–private cooperation in practice, unlike under the e-Evidence Regulation, requests for direct cooperation under the 2nd Protocol would not necessarily be binding: in relation to both domain name registration information and subscriber information, '[t]he form of implementation depends on Parties' respective legal and policy considerations'.²¹¹ In individual instances of cooperation, therefore, it will have to be ascertained whether cooperation across the territorial borders of parties is voluntary or mandatory, depending on the domestic arrangements of the party hosting the headquarters or representative of the service provider.²¹²

Second, at the 'higher' level, in the international setting differences in approach are routinely left in agreed texts in the form of explicit reservations or declarations – rather than being traded off or nuanced into a single compromise text, as is generally necessary for EU legislation. In its twin proposals for Council Decisions, respectively, on the signature and ratification of the 2nd Protocol, the Commission had envisaged instructing member states not to avail themselves of the two reservations listed above, but to ensure that they do make the declaration and notification listed subsequently, 'to ensure compatibility with the Commission's e-Evidence legislative proposals, including as the draft legislation evolves in the discussions with the co-legislators'.²¹³ By the time the final 'signature' decision was adopted, the EU Council had amended one of those two instructions: whereas Article 7.9.a (a general opt-out from direct disclosure of subscriber information) remained on 'refrain', in respect of Article 7.9.b member states were instructed that they 'may make such a reservation, but only in relation to access numbers other than those necessary for the sole purpose of identifying the user'.²¹⁴

That instruction was one of two main reasons why the European Parliament's rapporteur had proposed to reject the draft Council 'ratification' decision, for fear of different protection standards emerging inside the EU.²¹⁵ After agreement on the parallel EU e-Evidence reform had been reached, in January 2023 the European Parliament's Civil Liberties, Justice and Home Affairs (LIBE) Committee rejected the rapporteur's draft resolution, thus paving the way for the adoption of the Council decision and ratification of the 2nd Protocol by the member states on

²¹¹ See Council of Europe, *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (Explanatory Report to 2nd Protocol)*, ETS No. 224, 12 May 2022, para. 76 (domain name registration information) and para. 100 (disclosure of subscriber information).

²¹² In this sense, aspects of the 2nd Protocol can be viewed as an evolution of the 'soft law' of the T-CY Guidance Notes. See, in particular, Council of Europe, *T-CY Guidance Note #10: Production Orders for Subscriber Information (Article 18 Budapest Convention)*, [2017] T-CY(2015)16, 1 March 2017, and for criticism P. De Hert, C. Parlar and J. Sajfert, 'The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist Transborder Access to Electronic Evidence Promoted via Soft Law' (2018) 34(2) *Computer Law & Security Review* 327–336.

²¹³ European Commission, Proposal for a Council Decision authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence ('Draft 2AP Signature Decision'), [2021] COM(2021) 718 final, 25 November 2021, p. 9; European Commission, Proposal for a Council Decision authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence ('Draft 2AP Ratification Decision'), [2021] COM/2021/719 final, 25 November 2021, p. 9.

²¹⁴ Council 2nd Protocol signature decision, Annex, '1. Reservations'.

²¹⁵ The other main reason concerned the suspensive effect of notifications to 'local' parties under Art. 7(5a) 2nd Protocol. See European Parliament, *Explanatory Statement – Second Additional Protocol*, 12 January 2023, www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2023/01-12/Explanatorystatement-SecondAdditionalProtocol_EN.pdf.

the proposed terms.²¹⁶ The final opt-out dovetails with the final text of the e-Evidence Regulation, which explicitly assimilates traffic data that is ‘requested for the sole purpose of identifying the user’ to the less sensitive category of subscriber data.²¹⁷

3.4.2.2 To Be Continued: Future Impact on EU Data Protection Standards

The European Parliament’s rapporteur’s more specific concerns had been voiced against the backdrop of the weaker data protection standards currently applicable to certain (non-EU and non-Council of Europe) parties to the 2nd Protocol. At the same time, the protocol itself represents a variegated instrument of data protection harmonisation. Although it goes beyond the purposes of this chapter to attempt to gauge the likely impact of the 2nd Protocol (of which direct cooperation is only one aspect) on EU data subjects, a few remarks on the data protection-specific aspects of the reform may be instructive.

Article 14 is the relevant dedicated provision in the 2nd Protocol, setting out a suite of data protection principles and safeguards which correspond to those in the GDPR and the LED. These are purpose and use, quality and integrity, sensitive data, retention periods, automated decisions, data security and security incidents, maintaining records, onward sharing within a party, onward transfer to another state or international organisation, transparency and notice, access and rectification, judicial and non-judicial remedies, and oversight.²¹⁸

Here are certainly some notable iterations of the cornerstones of data protection law: for instance, parties shall not further process personal data for a purpose which is incompatible with the initial ‘*specific* criminal investigations or proceedings’;²¹⁹ a framework for dialogue between parties is in place aiming to accommodate the requirements of parties whose domestic legal framework requires ‘personal notice’ to the individual whose data has been collected (as opposed to the publication of ‘general notices’);²²⁰ and a party may suspend the transfer of personal data under the 2nd Protocol if it has substantial evidence that the other party is in systematic or material breach of the terms of Article 14 or that a material breach is imminent.²²¹

The last safety net has been included, the Explanatory Report notes, since ‘[t]he drafters considered that the safeguards of this article and their effective implementation are essential’.²²² By the same token, however, that aim is liable to be undermined by the limited scope of application of Article 14 itself. On the one hand, its contents can apply only to data received under the 2nd Protocol.²²³ On the other, it is disapplied in favour of ‘comprehensive’ mutually binding international agreements on the same matters or, if no such agreement is in place (so that they ‘retain flexibility in determining the data protection safeguards that apply to transfers between them under the Protocol’),²²⁴ parties may mutually determine that the transfer

²¹⁶ Council Decision (EU) 2023/436 of 14 February 2023 authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence (Council 2nd Protocol ratification decision), [2023] OJ L 63, 28 February 2023, pp. 48–53.

²¹⁷ See e-Evidence Regulation, Recital 32.

²¹⁸ 2nd Protocol, Arts. 14.2–14.14.

²¹⁹ Emphasis added; 2nd Protocol, Art. 14.2.a. in conjunction with Arts. 2.1.a. and 2.1.b.

²²⁰ Ibid., Art. 14.11.c.

²²¹ Ibid., Art. 14.15.

²²² *Explanatory Report to 2nd Protocol*, para. 282.

²²³ 2nd Protocol, Article 14.1.a. Parties remain free to apply higher standards to processing by their own authorities under Art. 14.1.e.

²²⁴ *Explanatory Report to 2nd Protocol*, para. 223.

of data under the 2nd Protocol may take place on the basis of other (not necessarily comprehensive, not necessarily binding) agreements or arrangements.²²⁵

For many parties, the relevant agreement is Convention 108 (and ‘108+’ where appropriate).²²⁶ Lack of space precludes a worthy analysis here of the ‘comprehensiveness’ of the modernised Convention 108 – in terms of both content and coverage – in the field of cross-border criminal investigations and proceedings, and of emerging direct cooperation powers in particular.

What remains to be specified, to close, is that the 2nd Protocol alone will have no effect on the application of the ‘Umbrella Agreement’²²⁷ between the United States and the European Union – as is confirmed in the Explanatory Report.²²⁸ From the opening in mid-2019 of negotiations in view of an EU–US agreement on cross-border access to electronic evidence for judicial cooperation in criminal matters, it has been common ground on the European side that the Umbrella Agreement clearly needs to be complemented with ‘additional safeguards that take into account the level of sensitivity of the categories of data concerned and the unique requirements of the transfer of electronic evidence directly by service providers rather than between authorities and transfers from competent authorities directly to service providers’.²²⁹ Once more, the ball is back in the Commission’s court.

3.5 CONCLUSION

This chapter set out to shed light on the relationship between EU data protection law and public–private ‘direct cooperation’ – in its multiple configurations, whether mandatory or voluntary – on digital evidence in criminal investigations. It built on well-established literature focusing on the transatlantic e-Evidence paradigm, as typified by the *Yahoo!* and *Microsoft Ireland* cases and the reforms launched in their wake, seeking to form a more complete view of relevant law and practice within Europe so that the data protection ramifications of the ongoing drive towards formalised and intensified mechanisms for direct cooperation may be better grasped. The scope of the analysis thus zoomed both further in and further out than the EU’s e-Evidence package and the US CLOUD Act. It zoomed in, for instance, by examining the legal regimes that apply where direct cooperation is of an entirely domestic nature but nonetheless triggers EU data protection law, and it zoomed out, for example, by broaching the future role of EU data protection standards in the Council of Europe’s own new direct cooperation facility, that of the Second Additional Protocol to the Budapest Convention.

The chapter detailed how the kinds of private-to-public data transfers for criminal investigations that used to fall (pre-GDPR) into the gap between separate regimes conceived respectively for private and public data processing are now subject to a degree of regulatory overlap. The *lex generalis* GDPR potentially applies whenever the *lex specialis* LED does not, and in some cases both instruments may apply. Given the discrepancies in the levels of protection afforded by the

²²⁵ 2nd Protocol, Arts 14.1.b.–c.

²²⁶ As mentioned in the *Explanatory Report to 2nd Protocol*, para. 222. See Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108 +), ETS No. 223, 10 October 2018. At the time of writing, twenty members and non-members of the Council of Europe (of which thirteen are EU member states) had both signed and ratified/acceded to the Protocol. Ireland has signed the Protocol, but not yet ratified it.

²²⁷ Agreement between the United States and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences (Umbrella Agreement), [2016] OJ L 336, 10 December 2016.

²²⁸ *Explanatory Report to 2nd Protocol*, para. 222.

²²⁹ Draft 2AP Signature Decision, 7–8; Draft 2AP Ratification Decision, 7–8.

two regimes, the question of which one is to apply to what stage(s) of any instance of public–private direct cooperation demands clarification. In taking up that gauntlet, the chapter distinguished between three scenarios of formal direct cooperation (along with one further scenario, that of informal or voluntary cooperation) and viewed those scenarios through the prism of data controllership.

Whilst the black-letter analysis revealed a hazy normative picture, with information on national implementations of the LED still fragmented, a conceptual-theoretical perspective identified several questions around the internal consistency of EU data protection law that remain on the table – despite the important contributions of the CJEU in recent years. Ultimately, the chapter argued that the bifurcated edifice of the EU data protection *acquis* continues to be fundamentally challenged by data processing that shifts between ‘public’ and ‘private’ realms, whether in isolated instances or in the course of more stable partnership-like arrangements, inherently engaging both GDPR and LED.

Most evidently, the purpose limitation principle risks being effectively emptied should data handled by private service providers slip from the ambit of the GDPR to the prosecutor, judge, police or other competent authority, operating (for core purposes) under the LED. Even if the position is assumed that investigative needs trump purpose limitation, this chapter has maintained that the effective fulfilment of data subject rights (and of independent supervision) can only be hampered by such levels of indeterminacy as regards the applicable legal regime(s).

The European Commission’s 2018 e-Evidence package did not engage with these questions, opting to refer to the EU data protection *acquis* in general. Had it explicitly engaged with the notions of data controller and data processor, this chapter posited, the criteria for joint controllership over the transfer may well have been met by the proposed scheme. The final text, released in January 2023, delivers a production order that is most aligned with the Council’s enforcement-oriented priorities, but containing elements of the Parliament’s mutual recognition-based vision. Although the question of the law that might apply to the transfer of digital evidence thus goes unanswered (is the e-Evidence Regulation to be considered the *passerelle* for data travelling from GDPR to LED?), data protection has not been lost in the wash: the new mechanism comes with a much-revised regime for the notification of data subjects. A first look suggested that both the wording of that regime and the transparency requirements related thereto could have been more finely tuned, so that in future it will be possible to precisely gauge the impact of the new reform on the effective fulfilment of data protection standards within the EU.

On Encryption Technologies and Potential Solutions for Lawful Access

Cyprien Delpech de Saint Guilhem

4.1 INTRODUCTION

In the eyes of the public, cryptography is likely imagined as that featured in the 2014 film *The Imitation Game*: pages of codes within Hut 8 and the clicking rotors of the Enigma machine. In fact, it has progressed significantly since this Second World War setting, and over the past seventy years it has developed into a modern science at the junction of mathematics, computer science and engineering, and touches every aspect of our daily digital lives.

With the fantastic rise of accessibility to the internet over the past thirty years, and, more recently, with the availability of personal computers and smartphones, we have seen a displacement of many aspects of our daily lives, both public and private, into the digital realm. Face-to-face interactions and verifications have been removed from many security and privacy-critical moments of our lives (such as transferring money or sending messages and photos to friends and family) and the intermediaries responsible for the communication and storage of sensitive information have become more complex and obscure. Both these developments should seem to contribute to an erosion of trust in the digital realm, but, counter-intuitively, this has not been the case; there has in fact been a rapid expansion of the range and the quality of digital services offered. Without the secure and efficient algorithms of modern cryptography that have been developed – concurrently to this expansion – to achieve a wide range of desirable security guarantees, many services today would not be able to operate as efficiently as they do or would not even exist at all.

Research in cryptography, from its very early days, has embraced the assumption that the inner workings of cryptosystems are public knowledge and known by potential adversaries.¹ In addition to confidence in the security of cryptosystems, this assumption has also helped build trust in such systems. Indeed, only when designs are accessible for scrutiny by independent experts and for debate by the research community can robust solutions emerge and gather both consensus and the backing of a majority for deployment. As a result of this process, strong encryption technology is now widely available in the digital world, both as blueprints and as usable software. This has many benefits, including the protection of information stored on devices and the security of, for example, payment information communicated over the internet.

¹ This is known as ‘Kerckhoffs’s principle’; it is named after Auguste Kerckhoffs who, in 1883, wrote two articles on cryptography in the first of which he lists six design principles for ciphers. The second of these principles requires that ‘[the system] should not require secrecy, and it should not be a problem if it falls into enemy hands’ (own translation). See A. Kerckhoffs, ‘La Cryptographie Militaire’ (1883) 9 *Journal des sciences militaires* 5–38 at 12. Another formulation, possibly independent, of the same principle was given by Claude Shannon as ‘one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them’: also known as ‘Shannon’s Maxim’. See C. Shannon, ‘Communication Theory of Secrecy Systems’ (1949) 28(4) *Bell System Technical Journal* 656–715 at 662.

To contextualise the current availability of this technology, as of 12 March 2022, between 86 per cent and 96 per cent (depending on the country) of pages loaded by users around the world of the Chrome internet browser used encryption by default (using the HTTPS protocol).² For context, in February 2022 the Chrome internet browser had a 63 per cent market share worldwide.³ This encryption covers all application data, that is, the content of websites (such as texts and images) as well as the input of the user to those websites (such as personal details, passwords, written posts and so on).

However, the public availability of such strong protection technology also causes problems when used by individuals who wish to cause harm to our societies. Secure messaging and the ease with which digital evidence can be concealed in plain sight using encryption are only two examples of how this technology can come to hinder the necessary process of law enforcement. This has resulted in heated debate on the use of such strong protection and on how the law enforcement process can continue to be exercised without hindrance when so much evidence remains inaccessible.⁴

This chapter aims to bring some technical explanation to this debate in an attempt to nuance the ‘all-or-nothing’ vision of encryption that has been put forward by some stakeholders engaged in this debate. First, it introduces the technology of ‘simple encryption primitives’ and explains how this can be used as a tool in wider programs and protocols to provide certain security guarantees. It also presents four areas where such protocols are used to provide confidentiality guarantees to different forms of data. Then it goes on to discuss other encryption technologies that achieve related, but different, security goals.⁵ While these are a long way away from being as widely used as the previous ones, they may give the reader an idea of the range of possibilities that modern cryptography can offer. Finally, the topic of lawful access to encrypted data is approached from a technological perspective; arguments against the need for (and use of) behind-the-scenes access are presented together with recent research ideas that may help bring about more targeted, secure and trusted solutions.

4.2 ENCRYPTION: STATE-OF-THE-ART

At its heart, cryptography is the science of information protection. While this originally meant only guaranteeing the confidentiality of data in transit by means of encryption, it now also covers additional desirable security goals. These include confidentiality⁶ of data in storage, integrity⁷ of

² Specifically, hypertext transfer protocol secure (HTTPS) encryption on the web. Google Transparency Report, transparencyreport.google.com/https/overview.

³ Browser Market Share Worldwide. StatCounter Global Stats, gs.statcounter.com/browser-market-share.

⁴ Europol, *The Internet Organised Crime Threat Assessment (IOCTA) 2015* (2015), 67–70, www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2015.pdf; Europol, *The Internet Organised Crime Threat Assessment (IOCTA) 2020* (2020), 21–22, www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf.

⁵ This chapter does not present other technologies of cryptography, such as digital signatures, zero-knowledge proofs or blockchains, which aim to provide different guarantees than confidentiality, such as authentication, integrity and public verifiability.

⁶ The term ‘confidentiality’ refers to the guarantee that data remains confidential, i.e., known only by the intended parties.

⁷ ‘Integrity’ means the guarantee that data has not been altered in any way between the time it was stored (or sent) and the time it was retrieved (or received).

data in transit and in storage,⁸ authentication⁹ of people and of data sources, and non-repudiation¹⁰ of communications, among many others.

This section first discusses the fundamental blocks of modern-day cryptography: encryption primitives. After then touching on the role these primitives play in larger protocol, it presents several applications of encryption, namely disk encryption, public-key cryptography and HTTPS traffic encryption, end-to-end encryption and the Tor network.

4.2.1 Encryption Primitives

The fundamental idea of modern cryptography is the displacement of trust, or of the burden of protection. Let us take the sending of sensitive messages as an example. Without cryptography one must trust that the messenger who is given the message will not cause the content of the communication to be revealed to the wrong people, or to the whole world, due either to third-party adversarial interaction or to the messenger's own negligence or even malicious intent. To prevent such a security breach, it is safer for the sender to place the message into a box, to lock that box using a special key and to send the box to the recipient for them to unlock it away from prying eyes. In this scenario, the sender needs only to trust that the recipient will not share the key that unlocks the box and that the box they use cannot be broken open in transit. Thus, the trust assumption is shifted from the messenger to the recipient's protection of the key, a situation which reduces the level of trust that is required of the sender, thus increasing security. Similarly, when one wishes to store data for a long time and not have to watch over it at every moment, the use of a box locked with only one key in the user's possession similarly displaces the burden of protection from the box to the key.

The above examples illustrate the technology of simple *encryption of data*, which secures the *secrecy* (or *confidentiality*) of a single given message, or a piece of information (also called a *plaintext*), by means of a *secret encryption key* (referred to only as a *secret key* or even *key* when the context is clear). This produces a 'locked box' called a *ciphertext*. It is the recipient's possession of the key that allows them to then *decrypt* the ciphertext they receive and recover the original plaintext. It should, however, be noted that this technology is capable of performing *only* the very simple task that it is designed to do – to encrypt a plaintext into a ciphertext using a secret key – and to do so only for small amounts of information at a time. Therefore, these small encryption algorithms are termed *cryptographic primitives* due to their fundamental and very targeted role.

Crucially, the assumption that the box cannot be broken open in transit illustrates the trust in the strength of the chosen encryption algorithm. This assumption is what enables the shift of trust from a communication channel that can be easily compromised on to the protection of the secret key used and to the strength of the algorithm.¹¹ Indeed, if copies of the key are made and

⁸ The term 'data in storage' (also sometimes 'data at rest') covers data that has been written to a long-term storage hardware, such as a hard drive, a portable universal serial bus (USB) drive, a disk or similar. 'Data in transit' refers to data that is being transmitted from one computer system to another, usually over a network which can be either private (like a company network) or public (like the internet).

⁹ 'Authentication' is a process which verifies a party's identity against a trusted authority; in the physical world, visually matching someone to the picture on their identity card, which is trusted since it is government-issued, is a form of authentication.

¹⁰ The term 'non-repudiation' refers to the inability of a party to claim that they were not the source of a communication that they in fact did emit; in the physical world, having impartial witnesses is a form of non-repudiation, as is the transcript of a court session.

¹¹ To illustrate this assumption in the context of law enforcement access to communications data, one could refer to the following example. Signal is a service provider whose encryption algorithm enables such a shift of trust in modern

handed around, then any person holding one is able to open the box and read the message; also, if a weak box is used, then it is easy for malicious parties to break it open and access the plaintext. It is, however, important to note that a key that unlocks one box does not provide its holder with any advantage to open another box that was locked with a different key – even if the two keys differ only by a minute amount and the two boxes were made in the same way. That is to say, if two plaintexts are protected using the same algorithm, but with two different keys, then knowledge of one key does not help in the decryption that requires the other.

The last decades of research in cryptography have shown that constructing trustworthy encryption algorithms is a challenging task, and many organisations have fallen victim to attacks because of their use of weak homemade cryptography.¹² As a result, several encryption algorithms have been standardised publicly, including the AES algorithm in 2001.¹³ The public component of such standardisation processes is crucial to guaranteeing the absence of any potential ‘back-door’ mechanism inserted by the designer.¹⁴ This guarantee then leads many companies and individuals to trust these algorithms as components of bigger systems which enable the wealth of digital services we see today. Indeed, despite being twenty years old, the AES algorithm is still considered to be one of the most secure encryption algorithms available.

It is important to stress that it is *not* a weakness for the design of such encryption algorithms to be public knowledge; the opposite in fact holds true. The standardisation process of governmental and non-governmental organisations, such as the USA’s National Institute of Standards and Technology (NIST) and the Internet Engineering Task Force (IETF), is typically carried out

digital communications. At the lowest layer, modern-day smartphones access the internet by connecting to a network (3G, 4G, 5G, etc.) using radio waves; these radio waves play the role of the ‘messenger’ in the metaphor used at the start of Section 4.2.1. The issue here is that such radio waves are a communication channel that can easily be listened to and recorded by anyone with the appropriate equipment. With its encryption algorithm that is executed on the user’s smartphone, Signal sends only ciphertexts over the communication channel. (This is, of course, a simplification: several other layers exist between the radio waves and the digital channel used by the Signal application.) These ciphertexts are assumed to be of no use to an eavesdropper who does not possess the secret key with which they are created and indeed, at the time of writing this chapter, the algorithm used by Signal remains secure. A second assumption is then that the secret key in question is well protected on the user’s smartphone. Often this is protected because the smartphone itself has device encryption enabled (a form of protection for data at rest) which protects its contents under yet another secret key, albeit in a very different manner.

¹² See, e.g., A. Greenberg, ‘Hackers Can Steal a Tesla Model S in Seconds by Cloning Its Key Fob’, *Wired*, 10 September 2018, www.wired.com/story/hackers-steal-tesla-model-s-seconds-key-fob/. In this instance the issue was due to a weak encryption algorithm being used by the key fob during its communication with the Tesla car. Given only two ciphertexts which were computed by the key fob as a function of its secret key, the researchers’ algorithm was able to re-compute the fob’s secret key, using a table of values computed ahead of time. Once the researchers’ device had recovered the secret key, it could use it to impersonate the fob when communicating with the car and thus unlock it and start the engine. This security breach was possible because of the weakness of the encryption algorithm: in short, its keys were too short and were thus simple enough to recover. With longer keys and a more secure algorithm, it is very unlikely that such a fast key-recovery attack would be possible.

¹³ Federal Information Processing Standards, *Advanced Encryption Standard (AES)*, Pub. No 197 (published in 2001, updated in 2023), <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf>. This standard specifies the Rijndael algorithm which was proposed by two Belgian researchers, Joan Daemen and Vincent Rijmen, in 1999 during the public AES selection process organised by NIST. The AES is now adopted worldwide as an encryption primitive present in numerous encryption protocols and software (such as the HTTPS protocol, see Section 4.2.4).

¹⁴ In both areas of software development and electrical engineering it is typically very difficult to reverse-engineer a finished product to work out what its function is. For example, given a software distributed by its producer as a program executable (e.g., an ‘.exe’ file), it is not possible to immediately recover a source code description of the program. Therefore, it is very difficult for outside observers to recover the whole intended function of the program. This means that a company could willfully embed malicious code in its software without appearing to. In the context of the design of the encryption algorithm, this means that a company could release software that, while genuinely encrypting the user’s plaintexts under their key, could also encrypt the same messages under the company’s secret key and send them to itself without the user’s knowledge. In the security community, such a hidden mechanism is termed a ‘back-door’.

over a length of time which allows for extensive analysis by the cryptography, security and engineering communities. This enables the development of algorithms that are fit for purpose and that stand the test of time. Furthermore, the public design permits continuous security assessment by the research community after standardisation, using new developments in attack techniques, which in turn allows for updated usage recommendations. These ensure that the encryption algorithms are used in the most secure way as soon as potential vulnerabilities are found. This enables software companies and digital services providers to update their cryptographic infrastructure and thus protect their customers' information from attacks.

That said, the public availability of robust standardised algorithms implies that the secrecy of encrypted data relies entirely on the secrecy of the encryption key itself. In many contexts where encryption is used, or other cryptographic techniques (such as digital signatures) that also rely on secret keys, it is up to the user to guarantee the secrecy of the keys used and great care is usually taken to ensure that these keys do not fall into the wrong hands. Another consequence of the design process of encryption algorithms is the fact that if two messages are encrypted under two different keys, then the successful decryption of the first, with or without knowledge of the corresponding key, does not yield any advantage for the decryption of the second.

4.2.2 *Encryption in Larger Protocols*

While the technology of encryption algorithms as presented in Section 4.2.1 may seem simple enough, it is crucial to note that it is described very far from its context and usage in current digital applications. As mentioned, the encryption algorithms whose behaviour are described, like the AES algorithm, are capable of *only* the very simple task of encrypting a plaintext into a ciphertext using a secret key. Furthermore, they are typically capable of processing only very small pieces of information; for example, any one of the AES algorithms can process only a plaintext the length of 128 bits at a time, which is exactly the length of the phrase 'Hello new world!' when represented as a series of zeros and ones. Thus, it is impossible to encrypt an entire file, let alone an entire computer hard drive, with a single execution of such an encryption primitive. To be able to process larger amounts of data, or to encrypt different kinds of information, these small and simple encryption primitives must be combined into larger *protocols* and *programs* which take care of preparing the plaintext information before encryption and of making the necessary ordered executions of the encryption algorithm. Such protocols and programs thus greatly diversify the use cases of encryption depending on their respective greater security goals.

After the design of the encryption algorithm itself, we have here another important security consideration. There are many ways in which the different executions of the algorithm can be combined to produce the final ciphertext corresponding to a large amount of data. Many of those ways are insecure, or create other undesirable vulnerabilities, and sometimes the confidentiality of the ciphertext can be broken without requiring a break of the encryption algorithm itself.¹⁵ The aforementioned protocols are often not the subject of standardisation, and it is from these

¹⁵ For example, it is not good practice to divide a file into sequential blocks of 128 bits and encrypt them individually and independently using the AES algorithm. Indeed, any 2 blocks of 128 bits that are the same within the file would produce identical ciphertexts after encryption. While this does not break confidentiality directly, it nonetheless reveals information about the encrypted file, namely, whether there are repeated blocks of data within it and where these are located within the file. In this case, a more elaborate way of chaining the data together must be devised, such as the AES-GCM algorithm (i.e., the AES algorithm executed in Galois counter mode), which prevents such information from being revealed.

designs that software companies and service providers hope to gain a competitive edge by promising better security constructions to their customers.

In addition to the composition of small encryption primitives in a secure way, these protocols are also responsible for creating and managing the secret keys used by the smaller components. To continue with the earlier example, the AES algorithms can use keys of 128, 192 or 256 bits in length (with increasing security guarantees for each variant) and, for better security, it is recommended that random keys are used.¹⁶ No human user can be expected to remember 128 (or more) random-looking zeros and ones in a row every time they wish to decrypt their files; therefore, the protocol must design a way to derive an appropriate key from simpler user-specific information, such as a password, a personal identification number (PIN) or even more identity-bound information such as fingerprints or even the user's face. (For ease of writing, we will refer to all such information as a user's 'secret'.) Furthermore, the protocol must be able to derive the same key every time the user presents their unique secret and ensure that a different key is computed if the wrong user attempts to access the system. This derivation method can again be subject to vulnerabilities, but it can also be capable of great flexibility and of providing different security guarantees and features.

4.2.3 Disk Encryption

A straightforward application of encryption technology is that of disk encryption for devices such as computers and smartphones. As more and more individuals are keeping sensitive and confidential private information on their many devices, which are at high risk of being lost or stolen, this technology enables strong protection against the increasingly bad consequences that these risks can bring. This technology unfortunately also enables individuals with malicious intentions to secure the digital content on their devices and prevent law enforcement agencies from accessing it.

In this context, a software component that encrypts and decrypts files is added to the device. This software derives the secret encryption key from the user's secret (e.g., passcode or password) and ensures that every file is encrypted under this key before it is written into the device's long-term storage. In doing so it ensures that were the long-term storage module to be removed from the device, then its content (or part of it) would be encrypted and indecipherable by anyone else.

There are different variants of such disk encryption software. Some are stand-alone programs and are not included within the operating system (OS) of the device.¹⁷ These typically encrypt only a specific set of files using the user's secret (which may differ from the one used to lock the device for access). These provide very strong security guarantees, not only because of the advanced encryption algorithms used but also because the safety of the files is directly tied to

¹⁶ While the term 'random' here may appear colloquial, the concept of randomness in fact holds a central role in modern-day cryptography. Its presence in everyday life may limit itself to the occasional flip of a coin (two possibilities) or perhaps the throw of a dice (six possibilities), but this kind of simple randomness is not sufficient to achieve cryptographic security. Indeed, if a secret key was as random as the flip of one coin, then any outsider would have a fifty-fifty chance of guessing the key correctly on the first try. Furthermore, it would take only two attempts to try every possible key. Instead, cryptography relies on secret keys with randomness comparable to the flip of (at least) 128 coins. While the increase from 2 to 128 coins does not seem much, this nonetheless gives rise to 2^{128} possibilities, i.e., 2 multiplied by itself 128 times. As a comparison, the age of the universe is estimated to be $2^{58.5}$ seconds. If one wished to attempt to decrypt a ciphertext encrypted with such a random key by trying every key, and one had a computer capable of computing 1 billion decryptions per second, it would still take more than 2^{39} times (approx. 550 billion times) the age of the universe to try every possible key.

¹⁷ For example: McAfee Drive Encryption, www.mcafee.com/enterprise/en-gb/products/technologies/drive-encryption.html.

the user's knowledge of their secret; often, no back-up of the secret or secondary recovery mechanism is available.

Other variants of disk encryption are seamlessly integrated with the device's OS; for example, this is the case with modern versions of macOS,¹⁸ iOS¹⁹ and Android.²⁰ Here, all of the user's files and sometimes the entirety of the device's long-term storage (except for essential start-up software) are encrypted using the user's secret. Such solutions are able not only to protect the content of the files but also to encrypt the metadata of such files (such as size, time of creation and modification, location on disk and so on). In this context, the encryption software typically relies on specialised hardware chips specifically designed to execute encryption algorithms like AES. This allows these devices to provide on-the-fly encryption and decryption of files between long-term and runtime storage at no performance cost noticeable by the user. To do this, the secret key derived from the user's secret can be kept in short-term memory for only as long as the device is used in that moment. Once the user locks the device up, the secret needs to be entered again to regain access.

It should also be pointed out that, in modern devices, the user's secret is usually not the only information required to derive the secret encryption key. Often devices are endowed with a unique identifier within their hardware which is also integrated with the key. This identifier can also itself be derived from the different physical hardware components, which means that changing part of the device could result in a different key and therefore prevent decryption from taking place, even if the correct user's secret is entered. This can be imagined as different parts of the device, such as the hard drive or the motherboard, having unique numbers scored into them when manufactured; these unique numbers are then used during the computation of the key when the device is configured. If someone then were to remove such a hard disk to place it in a different machine, the numbers would not match up with the rest of the system anymore and the correct decryption key would not be recovered. Even the software used by the device can be integrated into the key, which means that downgrading the OS to an alternative version could also result in a different key and prevent decryption. These checks typically happen at start-up when a device is powered on and help ensure that only the true user of the device can access the personal information that is stored within.

4.2.4 *Public-Key Cryptography and HTTPS Record Protection*

In the 1990s, with the rapid development of the internet and its potential to become a global network, it became important to create solutions to ensure the confidentiality and authenticity of communications. Indeed, it quickly appeared that such a network had great potential for sensitive communications such as payment information for online shopping, sending personal emails and accessing online banking information. Given the private nature of these communications, it was important that systems were designed to ensure their security. The first of these was the Secure Sockets Layer (SSL) protocol proposed by Netscape in 1995,²¹ which rapidly evolved into the Transport Layer Security (TLS) protocol, first standardised by the IETF in 1999.²² Nowadays, TLS 1.2 is the most widely used protocol to secure internet communications within

¹⁸ Apple Inc., 'About Encrypted Storage on Your New Mac', 6 November 2018, support.apple.com/en-us/HT208344.

¹⁹ Apple Inc., 'Encryption and Data Protection Overview', May 2021, support.apple.com/en-gb/guide/security/sece3bec0835/1/web/1.

²⁰ Android, 'Encryption', Android Open Source Project, 6 June 2022, source.android.com/security/encryption.

²¹ K. Hickman, 'The SSL Protocol', 9 February 1995, tools.ietf.org/html/draft-hickman-netscape-ssl-00.

²² T. Dierks and C. Allen 'The TLS Protocol Version 1.0', January 1999, tools.ietf.org/html/rfc2246.

the HTTPS protocol (where the ‘S’ stands for ‘secure’). The latest iteration of this process, TLS 1.3, was standardised in August 2018.²³

This family of protocols is designed to enable two parties, usually referred to as ‘the client’ (representing individuals using their computer at home) and ‘the server’ (representing companies hosting websites available for users to access), to establish and communicate over a secure channel. Here the term ‘secure’ first means that the content of the communication sent over the channel is protected by the protocol using an encryption algorithm such as AES. It also usually means that the server is authenticated to the client, that is, the server must prove its identity before the channel can be considered established. The combination of the two guarantees ensures that only the recipient intended by the client can read the information sent over the communication channel, that is, the internet. The development of these protocols was a major contributor to the rapid expansion over the last two decades of online commerce and of services dealing with private information such as online shopping (e.g., Amazon), email communications (e.g., Yahoo, Gmail) and online banking (e.g., Home’Bank by ING Belgium).

4.2.4.1 Public-Key Cryptography

The need to establish encrypted communications over such a large network presented cryptography with a new technical challenge. Up until this point, this chapter has presented forms of encryption where the key used for decryption was the same as that used for encryption. These forms of encryption allow for very fast algorithms, but they come with a big disadvantage: when encrypting messages, the sender and the recipient both need to hold the same secret key to communicate. While this may be feasible within organisations where copies of keys can be given to members (on a USB key or on a smartcard), this is not possible when parties who have never met wish to communicate. For instance, it would not be possible for Amazon to send a physical smartcard to each of its clients for them to use when communicating their payment details. Therefore, there is a requirement for clients and servers to transition from a state of communicating over an insecure channel to one of having established a shared secret key which allows securing the channel from that point on.

Cryptography has been able to provide a solution to this requirement since the seminal 1976 paper of Whitfield Diffie and Martin Hellman.²⁴ This work introduced a different form of encryption, known as *asymmetric* (or *public-key*) encryption, as opposed to the kind discussed earlier, known as *symmetric* encryption, where parties are assumed to each hold a copy of the same key.

In asymmetric cryptography, each key is divided into two separate, but mathematically related components, a public one and a private one. In the context of encryption, the public key is used for the encrypting procedure only, and therefore can be revealed to the world safely, hence its name. With such a system, anyone can encrypt a plaintext with a recipient’s public key and send them the ciphertext. In addition, this method of encryption provides security guarantees of the same level as those provided by symmetric algorithms.

To decrypt ciphertexts generated in this way, a recipient must hold the private key bound to the public key that was used during encryption. This private key is used only for decrypting such ciphertexts and therefore it must be securely kept in the same way as symmetric keys, but it does not need to be shared for two parties to securely exchange information. Each party can generate

²³ E. Rescorla, ‘The ‘TLS Protocol Version 1.3’, August 2018, tools.ietf.org/html/rfc8446.

²⁴ See W. Diffie and M. Hellman, ‘New Directions in Cryptography’ (1976) 22(6) *IEEE Transactions on Information Theory* 644–654.

his/her own public and private key pair, exchange their public keys and proceed to securely communicate using public keys for encryption and private keys for decryption. A useful illustration may be that of an imaginary special kind of lock and key where anyone can create a new (private) key and then create many copies of a lock (public key) that can only be opened by that private key. One would then distribute these unlocked locks to everyone who wished to communicate with them, and these locks could be locked by the sender at the moment of sending, representing encryption using the public key. When the creator of the key received a message locked using one of these locks, they could then use their special private key to unlock (i.e., decrypt) the message.

A crucial assumption in this context is that it is very difficult for someone to recover the private key that lies behind a given public key. In cryptography, the meaning of ‘very difficult’ is carefully defined and parameters for public-key encryption algorithms are accordingly chosen such that this assumption can be trusted. This comes in addition to the assumption that the encryption algorithm itself is secure, but here again transparent standardisation processes and the public availability of research on the hardness of key-recovery problems provide strong confidence.

Unfortunately, the drawback of even the most efficient public-key encryption algorithms is that the mathematics employed for security come with a cost to efficiency. Either computation time for encryption and decryption can be slow (too slow for realistic deployment on the internet – web pages would take several seconds or even minutes to load, similarly for encrypted messages like WhatsApp) or the amount of information that is necessary to communicate needs to be greatly increased (each symbol of plaintext may transform into many symbols of ciphertext to the point where a simple email could become as large to send as a song or even a movie). While it would be reasonable to suppose that, with computers getting faster every year, these drawbacks would eventually be removed, it is important to point out that faster computers also mean better attack capabilities, which in turn require stronger parameters to be mitigated and again create higher efficiency costs.

4.2.4.2 HTTPS Record Protection

The solution to this drawback has been to combine both kinds of cryptography, symmetric and asymmetric, within protocols to achieve efficiency for real-world use cases. Every secure channel established with the TLS protocol, used within the HTTPS protocol,²⁵ begins with a *handshake protocol* in which public-key cryptography is used briefly to enable the parties to jointly establish a short secret key known to both. Using our private key–public lock analogy of before, such a handshake could proceed as follows: a client wishing to connect to Amazon first asks Amazon to send them a public lock. Next, they create a random secret key and lock it with Amazon’s public lock; they then send this locked message back to Amazon. As Amazon knows the secret private key of all its public locks, it can open the message and recover the client’s secret key. From that point on, Amazon and the client share the same secret key and can use it to secure their communication, instead of the public-lock system.²⁶

²⁵ R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach and T. Berners-Lee, ‘Hypertext Transfer Protocol – HTTP/1.1’, June 1999, tools.ietf.org/html/rfc2616; E. Rescorla, ‘HTTP Over TLS’, May 2000, tools.ietf.org/html/rfc2818.

²⁶ Note that the analogy presented here is in no way an accurate representation of the current state-of-the-art for such handshake protocols.

This process, known in cryptography as *key agreement* or *key transport*, provides many of the security guarantees expected from a secure channel, especially the guarantee that the secret key is known only to the client and the intended server, and to no one else. This handshake ensures that the use of public-key cryptography, expensive in terms of both computation and communication, is kept to a minimum. Once the secret key is established at both ends by the handshake protocol, the *record protocol* then uses it to encrypt and decrypt messages exchanged between the client and the server with symmetric encryption, thus adding the confidentiality and integrity guarantees provided by these algorithms.

While the encryption protection described just now may seem to provide many security features, it is important to note that the HTTPS protocol sits only at the highest level of the protocol stack in internet communications. By this we mean that it is the front-line protocol that a client web browser uses to communicate to a server and there are several other protocols that come after it even before the information can leave the client's computer and be sent over the internet. For example, this means that the destination information (such as the website domain name or the internet protocol (IP) address of the server), or other such *metadata*, cannot be encrypted within the record layer, as otherwise the lower layers would not know where to send the information over the network. The metadata must therefore be communicated in clear (i.e. without encryption) and is vulnerable to eavesdropping. In our earlier analogy of sending encrypted messages being like sending a locked box by messenger, it is intuitive that the messenger still needs to know the intended destination of the box even if he/she cannot access its contents. Therefore, if that messenger is intercepted and questioned, the intended destination can still be revealed to third parties. As a more concrete example of how this can manifest in modern internet communications, this is how service providers are able to selectively block their clients from accessing certain websites, like those which enable the pirating of copyright-protected material. Even though these providers are not able to view the content of the communications protected by the record layer, they can still prevent the sending and receiving of messages if they see, in clear, that they come from a certain source. Such metadata can also include geographical location and time information. Similarly, the quantity of content that is transferred through the record layer is not hidden because the data is broken down by the lower layers into little packets that are sent over the network individually, one after the other. This helps to prevent large amounts of data being lost in transit over the network or received in the wrong order. Thus, traffic analysis of a client's communication can easily reveal whether they are reading the news, browsing social media or watching a film, even if the specific content of the pages (the text in the articles, the pictures shared by friends, the images of the film) remains hidden from outside view.

Similar encryption technology is also used to create virtual private networks (VPNs) which allow users to connect to a private protected network over a public (unprotected) one. In this context, a secure channel (sometimes referred to as a 'tunnel') is established between the client machine and a gateway server that is an entry point to the private network. When the client wishes to communicate over the private network, it sends its message, including the metadata, through the tunnel which protects it from outside view. The gateway server then acts as the client towards the rest of the network and relays the original client's message; when it receives a response from the network, the gateway server relays it to the client through the secure tunnel. This is used in enterprise settings where users wish to access the private network when they are out of the office. Thus, from an outsider's perspective, it only seems that the user is communicating with the entry server through the secure tunnel, whereas it in fact could be communicating with many others with the server acting only as a relay.

It could also be that the user accesses the public internet through such a VPN. In this context, the user would be directly communicating only with the relay server and the relay server would be communicating to the internet. This allows, for example, accessing location-restricted services (e.g., geo-locked content such as the BBC's iPlayer service which is available online only in the UK) from anywhere by accessing a gateway server that is itself located in an authorised location.

In other words, the only metadata available to outside observers, such as the internet access provider, relates to the user's access to the internet through a VPN and information concerning this VPN connection, such as the location of the servers running the VPN software. When such connections are used to access the internet of a foreign country via a VPN, all the metadata regarding the real connection of the user is only revealed within the servers of the VPN service situated in this foreign country.

4.2.5 *End-to-End Encryption*

In recent years, especially after the so-called Snowden revelations,²⁷ it became widely recognised that apparently private online messaging conversations could be read in clear by the platform providers and that these could be passed on to law enforcement. Seeking other solutions, privacy-concerned individuals turned towards the Signal protocol,²⁸ which offers the guarantee of *secure messaging* via the technology of *end-to-end encryption*. It is this same protocol that was then adapted by service providers for other popular messaging applications such as WhatsApp.²⁹

Here, 'end-to-end' means that, during a conversation, the message is first encrypted directly on the sender's device before being sent, as a ciphertext, to the platform provider's servers over a secure channel. In a second stage, the message is delivered to the recipient's device, still as a ciphertext, and only then is decrypted for the user to read. As always with encryption, the security of the ciphertext is directly linked to the security of the key that is used for encryption. The crucial security aspect of end-to-end systems is that the key is known only to the sender and the recipient, and *not* to the service provider's servers, which may store the ciphertexts for some time while awaiting delivery. As the platform provider is now unable to read the conversation of its user in clear, it is also unable to pass it on to other parties. Only the parties possessing the key, that is, the sender's and the recipient's devices, can access and display the message.

To establish such a channel between one end, the sender's device, and the other, the recipient's device, a similar process is used as during HTTPS connections. First, asymmetric cryptography is used to establish a shared secret key between the two devices, using the parties' public and private keys, and then symmetric techniques are used to encrypt the content of the communication. The crucial design aspect used to provide end-to-end security is that the service provider's servers are not included as parties in the key exchange between the two devices. While these servers may be used to facilitate the exchange, for example by temporarily storing protocol messages if one device is disconnected from the internet when the other attempts to initiate a conversation, their public keys are never included in the creation of the shared symmetric key, thus preventing them from obtaining any knowledge about it. Only the sender's and the recipient's devices, which know their own private keys, may derive the secret key required for

²⁷ S. Landau, 'Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations' (2013) 11(4) *IEEE Security & Privacy* 54–63.

²⁸ Signal, signal.org.

²⁹ M. Marlinspike, 'WhatsApp's Signal Protocol Integration Is Now Complete', Signal, 5 April 2016, signal.org/blog/whatsapp-complete.

encryption and decryption. Importantly, such private keys are also never backed up to the service provider's servers, meaning that they are unable to provide them upon request. While this may be a drawback for law enforcement authorities which seek to get access to the content of a suspect's communications, it guarantees that any compromise of the service provider's servers by hackers does not accidentally reveal the communications of all its users, as the provider does not have any means of accessing the messages.

There is an additional design aspect of end-to-end encryption protocols that marks the difference with those used for HTTPS client-server communication. For the latter, the secret symmetric key is first established at the opening of the secure channel (during the handshake) and then used, unchanged, throughout the session until the closure of the channel (when the client closes his/her browser). However, for the former, the symmetric key is continuously updated as the channel is used, in most cases with every new message, in a process called *ratcheting*. Here, the mathematics of public-key cryptography are leveraged to provide a continuous key exchange process that takes place in parallel with the conversation over the end-to-end encrypted channel. This updates the symmetric key used, injecting new randomness with every message and including information related to previous messages and keys from the same conversation to maintain integrity, making sure that someone who does not have access to the conversation history cannot begin intercepting.

This process is more complex than that of simple secure channel establishment for HTTPS connections, but this is required by the different deployment contexts of these protocols. Indeed, messaging conversations tend to have a much longer lifespan than browser-server connections, sometimes going on for months, and it is important that the confidentiality of messages is preserved throughout, even in the event of compromise. Ratcheting provides security guarantees known as *forward-security* and *backward-security*, which protect messages in the past and in the future against leaks of encryption keys in the present. Thus, if the current encryption key for a conversation is compromised at one of the devices, the ratcheting mechanism prevents this from leaking any information about previous or future messages by continuously updating the key with new randomness. This drastically complicates the strategy for a potential attacker as they would have to obtain every new encryption key, created with every message, to read the conversation in clear. If users furthermore delete messages after a short period of time, even malware on the device would not be able to recover past conversations via other means; the only way of attack would then be to decrypt stored ciphertexts (if an attacker had stored them while eavesdropping), knowing that every ciphertext is encrypted under a different key due to the ratcheting process.

It is important to note here that, similar to HTTPS connections, metadata is not protected by end-to-end encryption, only the content of messages is. Therefore, information such as the identities of sender and receiver, their location, the number of messages sent and received, timestamps and so on can be inferred from the protocol messages sent by the devices. If these communicate with the service provider's servers in between them using a separate secure channel, this metadata is protected by that channel, but the service provider itself can access it.

4.2.6 The Tor Network

Another example of the use of encryption to guarantee freedom of access to services and the confidentiality of personal information is the Tor network, named after its original software

project ‘The Onion Router’.³⁰ This network is used by users who wish to keep their location and traffic behaviour, in addition to the content of their communications, hidden from eavesdroppers and traffic analysis.

To achieve this, when a user wishes to send a communication over Tor, their browser first selects a random list of ‘relay nodes’. These are computers that have been configured with public software to be part of the volunteer Tor network distributed all over the world.³¹ As indicated by the acronym, the plaintext communication of the user is then packaged similarly to an onion: using several layers of encryptions one after the other such that the outermost layer is encrypted with the first relay node’s public key, and the innermost layer is encrypted using the last relay node’s key. Then, the communication travels through the list of relay nodes with a layer of encryption being ‘peeled’ off at each node before being passed on to the next one.

In this way, each node only learns the next node in the chain by peeling off one layer of the onion (i.e., decrypting the packet) and passing it on. None of the nodes can see the destination of the plaintext packet except for the last one, called the ‘exit node’, as it now passes the packet forward over the internet. It should be noted that the plaintext packet is in fact often a TLS-protected message and is therefore also unreadable even to the last node, which can only learn where that message is headed (i.e., the message’s metadata). By also not including origin information in the packets, except in the one destined for the first node, the user hides its own identity from all the other nodes in the chain. Even the destination server of the plaintext packet cannot trace the original user. That final server can of course identify the exit node used by the packet (i.e., the point at which it left the Tor network), but the server can also see that the communication took place over the Tor network and therefore infer that the exit node is not the true sender of the packet.

As with all security systems, the Tor network can be very powerful when configured correctly. There are many scenarios in which incorrect configurations can leak information that the protocol instead aims to protect. These leaks are rarely due to weaknesses in the encryption algorithm itself, as the protocol is kept up to date and ensures the correct use of algorithms, which still guarantees that the content cannot be decrypted. Instead, these leaks are often due to the way that metadata can be inferred by analysing correlated behaviour. For example, by casting a sufficiently wide net over the nodes of the Tor network – which the number of nodes makes a challenging task – it may be possible to gather information on a packet as it bounces from one node to another to eventually learn which entry and exit nodes are connected, and therefore obtain information (time, place, identity and so on) on the original sender of the communication. To perform such information gathering typically requires specific deployment of monitoring technologies combined with statistical analysis.

4.3 ADVANCED ENCRYPTION TECHNOLOGIES

In Section 4.2, we presented symmetric encryption primitives and four applications in which they have been deployed to protect the confidentiality and integrity of information. In each of them, the cryptography is kept as simple as possible because efficiency is key in deployed protocols to maintain high speeds of communication. Due to decades of improvement in cryptography, programming and engineering, the current solutions provide a very performant

³⁰ Tor Project, FAQ, <https://support.torproject.org/about/>.

³¹ At present, there are between 6,000 and 7,000 active relay nodes on the Tor network (<https://metrics.torproject.org/networksize.html>). The owners of these nodes are not publicly listed, but any individual or company can choose to execute the publicly available software required to run a Tor relay node.

combination of security and speed while also keeping the trust of the security-minded communities that contribute to their development and their deployment. That trust furthermore comes from the design of the protocols which prioritise one strong security goal, confidentiality, without compromise. As such, and given the wide adoption that they benefit from, it is fair to say that the current solutions are unlikely to be replaced in the near future.

Research has, however, led to alternative, more advanced encryption technologies where different aims are considered. These other solutions, while sometimes as efficient as the widely deployed symmetric and asymmetric techniques, may often be too complex or too specialised in their capacities to be adopted by a wide community of users, but they may interest smaller groups, such as companies or public services, where a dedicated solution is required. The interest of these technologies is that they aim to go beyond the obvious requirement of confidentiality. They aim to answer the question ‘Now that data is encrypted, what can be done with it?’. For example, fully homomorphic encryption and multi-party computation, which will be discussed in Sections 4.3.1 and 4.3.2, respectively, are different but related technologies that enable computation on encrypted data. Such computation could be anything from simple addition to complex machine learning operations and include targeted access to and analysis of encrypted data.

In the context of access to encrypted data for evidence purposes, the current application of these techniques is limited since systems of interest were not conceived to be compatible. However, one can imagine future systems where compatibility with evidence gathering is envisaged and studied from the start by, for example, building these advanced technologies into the systems of interest. Here again, the question of trust arises, and a transparent design process of such systems would be necessary to build consensus around their deployment. In what follows, we will focus on three of these more advanced encryption technologies and briefly explain their potential, including for law enforcement and other authorities.

4.3.1 *Fully Homomorphic Encryption*

In recent years there has been an intense development of cloud services that provide storage or computation power to users from a remote location. While this solution often benefits clients who need to store and compute large amounts of data, it also requires the clients to trust the company providing these services. Indeed, the ‘cloud’ is nothing more than a large number of servers owned by the provider, connected to the internet and stored in a large facility somewhere in the world. As such, anything stored on them in an unprotected manner is always visible for at least the cloud provider itself, if not also for other parties such as law enforcement agencies of the territory where the provider is located.

It is in this context that the technology of fully homomorphic encryption (FHE)³² aims to bring solutions. This particular form of encryption enables mathematical operations to be performed directly on ciphertexts, without knowledge either of the underlying plaintext or of the encryption key. The mathematical design of the primitive then guarantees that the operation performed on the ciphertexts yields a new ciphertext which encrypts the result of the operation performed on the corresponding plaintexts. With such a scheme, one could, for example, add an encryption of two to an encryption of five and obtain an encryption of seven without knowing, or learning, what any of these numbers were. While this only exemplifies an addition, any

³² For more on this, see F. Armknecht, C. Boyd, C. Carr, K. Gjøsteen, A. Jäschke, C. A. Reuter and M. Strand, ‘A Guide to Fully Homomorphic Encryption’ (2015) *Cryptology* ePrint Archive 1–35, <https://eprint.iacr.org/2015/1192.pdf>.

operation can in fact be performed. Therefore, complicated computation can be performed using such schemes while maintaining complete confidentiality of the underlying data. This can be applied to sensitive medical data, for example, by having a person's genome encrypted with FHE and using the computational power of cloud services to perform in-depth analysis without having to share confidential information.

This would be very valuable for users who require enormous amounts of data to be processed as they would be able to encrypt it all, place it on a cloud provider's servers and let them perform the processing directly on the encrypted data. The users would then receive the result, still in encrypted form, and decrypt it with their own key. However, while great progress has been made in recent years, such encryption technology still comes with a cost in communication and computation time that is much greater than traditional symmetric and asymmetric encryption technologies and, at the time of writing, still too high to enable deployment on a global scale. As of now there are therefore no widely deployed FHE-based solutions available for users.

4.3.2 Multi-party Computation

Another need for cryptographic solutions arises when multiple mutually distrusting parties require each other's private information to perform a computation. For example, a doctor with a patient's magnetic resonance imaging (MRI) results may wish to have them analysed by a hospital's highly performant algorithm. However, the patient does not wish for their scan to become part of the hospital's database, and the hospital does not wish to share its algorithm due to the risk that the doctor will then use it for their own gain. The technology of multi-party computation (MPC) provides a solution to this challenge.³³

In MPC, each party brings its own private information to the computation and securely shares it among all the participants in such a way that the information cannot be reconstructed unless a defined group of participants decides to collude. The information is also shared in such a way that it is possible to compute with it and obtain a securely shared form of the result. Only by engaging in this process all together can participants obtain the assurance that the computation was correctly executed and that their secrets were not revealed to the other participants.

This technology can, for example, allow states to compute statistics on their joint census data without having to share them with each other, or allow government agencies to analyse companies' data without having access to the data itself. For example, this could include statistical analysis of financial flows to detect fraud or other suspicious activity across the data of several participating entities. It is important here to note that all the participants must agree on the computation that is to be performed and that it is not possible for one of them to obtain a result that is not intended by the others.

4.3.3 Attribute-Based and Searchable Encryption

Among other ways in which encryption primitives have been developed to address secondary goals are attribute-based encryption (ABE)³⁴ and searchable encryption.³⁵ The first of these two,

³³ For more on this, see R. Cramer, I. Damgård and J. Nielsen, *Secure Multiparty Computation and Secret Sharing* (Cambridge: Cambridge University Press, 2015).

³⁴ For more on this, see A. Sahai and B. Waters, 'Fuzzy Identity-Based Encryption' (2005) *Annual International Conference on the Theory and Applications of Cryptographic Techniques* 457–473, https://link.springer.com/content/pdf/10.1007/11426639_27.pdf.

³⁵ For more on this, see C. Bösch, P. Hartel, W. Jonker and A. Peter, 'A Survey of Provably Secure Searchable Encryption' (2015) 47(2) *ACM Computing Surveys (CSUR)* 18–51.

ABE, aims to design an algorithm in which attributes possessed by a user determine whether they can decrypt a given ciphertext or not. Such attributes may be a user's email address, their age, their gender, their profession, their job title or any other such information; these are then inserted within a user's key when it is created. When one wishes to encrypt a plaintext only for a certain group of users, they can include a policy component to their ciphertext which describes the attributes that are required for decryption. For example, in a company, one could encrypt sensitive documents under the policy 'only for employees of department X' or 'only for employees of rank greater than or equal to Y'. When users wish to decrypt such a ciphertext, they will be able to do so only if the attributes contained in their key match those required by the policy; if they do not, the user will not be able to recover any information from the ciphertext. In this context, users should not be trusted to generate their own keys as they could insert attributes that they do not legitimately possess. Instead, ABE requires a trusted central authority in the system to distribute users' keys to them. That authority can then be trusted to verify attributes by some other method and to give out keys that contain only the correct ones. However, this authority must also be trusted not to abuse its power since it learns all the users' keys in the process. This strong trust requirement is a significant obstacle for the deployment of ABE for generic purposes as users will typically not be able to all trust the same authority. For example, deploying an ABE system over the entire internet, which would allow for attributes such as age or profession to be considered for encryption policies to restrict content to only certain populations, would require all internet users to trust a single authority. Given the diversity of individuals worldwide, this would be very challenging.³⁶ Nevertheless, ABE technology may be more fit for purpose for comparatively smaller use-cases such as companies where all employees can trust their central information technology (IT) department, or for government services where citizens are assumed to trust their government, especially when the technology is used to facilitate access to data that the government already knows or already provides to certain categories of citizens. For example, medical records could be protected with such a scheme and made available to doctors (with the patient's consent) whose keys would be configured by a central authority; similarly, access to fiscal records of citizens could be protected and controlled in this way.

Next, searchable encryption is similar to FHE and MPC in that it aims to retain certain computation abilities once the plaintext is encrypted. This type of encryption aims to provide the user with the capacity to search through the ciphertexts using a keyword to quickly recover plaintexts of interest. An efficient solution for this challenge would allow for entire databases to be kept encrypted and for search queries to be computed without having to decrypt the entirety of the data. For example, an entire health-care system's database of patient records could be encrypted and stored while at the same time allowing doctors to search for specific patients or other keywords to retrieve the appropriate records. To achieve this, such primitives encrypt both the plaintext and a series of token keywords that represent this plaintext. The encryption of the keywords themselves is crucial to not reveal information regarding the plaintext. When users wish to submit a query, they encrypt the keyword that they are searching for, and a comparison is made to return the ciphertexts that match this encrypted keyword. While this may seem simple enough, this solution can be vulnerable when related queries are asked in succession (e.g., when someone searches for two names that are close to each other in alphabetical order, they could learn whether other names are present in between in the database; this reveals more information

³⁶ Moreover, it should be noted that it may not be desirable to allow content providers to enforce such blatant discrimination onto their users.

about the database than intended by the system) and more security measures usually need to be deployed around this primitive to prevent misuse of the system.

4.4 TECHNOLOGICAL SOLUTIONS FOR LAWFUL ACCESS

With the rapid expansion of the availability of encryption technologies, fuelled by progress in computing speed and protocol developments such as those mentioned above, there has been an equally rapid growth of requests from law enforcement agencies or other government authorities to access encrypted information that would be important to criminal cases.³⁷ When faced with encryption, law enforcement agencies typically have three options: to obtain the secret key directly from the user, to obtain the information from a service provider if such access is possible, or to circumvent or break the encryption technology.

While investigating officers may sometimes be lucky enough to find a device unlocked or a password written down, the first option above usually relies on the user giving up their knowledge of the secret. Yet, whether the latter is acceptable is more a question of law, related to the right against self-incrimination, and is not addressed in this chapter.

The second option relies on the service provider having access to either the information or the secret key and being willing to cooperate with the authorities. This situation happens with mobile phones, for example, where telecom operators can store databases of keys linked to subscriber identity module (SIM) cards and are able and willing to share specific keys with law enforcement agencies when required. However, with the widespread deployment of encrypted calling and messaging technologies over the internet, such as the end-to-end encryption discussed in Section 4.2.5, the companies behind these communication tools are now technically unable to provide this access.

The third and last option is now the one causing the biggest problems for law enforcement agencies. With the advancement of encryption technology and the diversification of its applications, circumventing or breaking it has become nearly impossible. This diversification is, for example, demonstrated in Europol's latest Internet Organised Crime Threat Assessment (IOCTA) report where the organisation highlights the problems linked to encryption of DNS queries, which amounts to a form of metadata encryption (so not only is the content data encrypted but so is the data concerning the website that is accessed).³⁸ Regrettably, it appears that governments are still very much centred on enhancing decryption capabilities during police and criminal investigations, as demonstrated by the recent launch of the Europol decryption platform,³⁹ and not considering alternative solutions. According to the press release, 'Europol's European Cybercrime Centre will operate the platform and leverage its in-house expertise in

³⁷ See, e.g., J. Cox, 'Encryption Gets in the Way of 75% of Cases, Europol Chief Says', *Vice*, 10 May 2016, www.vice.com/en/article/4xa3jq/encryption-gets-in-the-way-of-75-of-cases-europol-chief-rob-wainwright.

³⁸ Domain Name System (DNS) queries are requests performed by web browsers when a user wishes to access a website. To obtain the content required to display a website, the web browser must know the IP address of the server where this content is hosted. However, human users are not expected to remember IP addresses and so the DNS offers a translation service between domain names (such as 'ecosia.org') and the corresponding IP addresses. According to Europol, observing a history of DNS queries (i.e., a history of the websites that a device has asked to visit) helps investigate criminal behaviour. The recent development of DNS over HTTPS (DoH) now allows for these DNS queries to be encrypted and thus avoid scrutiny. See footnote 4.

³⁹ Europol, 'Europol and the European Commission Inaugurate New Decryption Platform to Tackle the Challenge of Encrypted Material for Law Enforcement Investigations', 18 December 2020, www.europol.europa.eu/newsroom/news/europol-and-european-commission-inaugurate-new-decryption-platform-to-tackle-challenge-of-encrypted-material-for-law-enforcement.

providing the most effective support to . . . investigations'; this does not promise much public information regarding which processes will be used to perform the decryption in question.

This final section discusses some of the issues with behind-the-scenes access to encrypted data. It also looks at technological alternatives that could be put in place instead in an effort to move away from the unsustainable cycle of ever stronger encryption driving ever stronger decryption and vice versa.

4.4.1 *Issues with Behind-the-Scenes Access to Encrypted Data*

It is important to note that the idea of back-door access stands at odds with what has made cryptography so trusted and reliable in recent decades. A hidden and unregulated back-access into a security-sensitive data protection mechanism does not make sense when we recognise that the strength of such modern protection mechanisms comes from transparent and publicly available standardisation processes as well as constant public research and development.⁴⁰ The risk with hidden access mechanisms is either that governments will eventually lose control of them (e.g., because of rogue employees or hacks from outside criminals) or that hackers will eventually discover the vulnerability itself and reverse-engineer a method to exploit it for criminal gain. The public processes and continuous research ensure, if only from a technical point of view, that the security claims made by algorithms and protocols are indeed valid and that, to the best of cryptography's current knowledge, hold strong against almost all efforts to circumvent them. As exemplified previously, there have been occasions where in-house secret cryptography has been broken under the scrutiny of experts, and others where, despite a wide community's best intentions, progress of attack methodologies has meant that what used to be secure no longer is, and therefore that the recommendations for use must change. This flexibility in ensuring that security as promised is always delivered to users is not possible in systems which are maintained with different goals in mind, such as the constant possibility for alternative access to protected content. Furthermore, with the series of recent revelations concerning state agencies' mass surveillance practices, individuals are now acutely aware of the risk that their private information may be monitored in permanence and therefore tend to favour solutions which emphasise data protection and privacy. As a result, it is not in many service providers' interest to comply with governments' request for back-door access as that would drive users towards other providers with better solutions.⁴¹

Protection of individuals from unrestricted access from their own government is not the only serious concern of generic back-door access within encryption technologies. Globalisation now means that many online service providers have users all around the world while their headquarters remain located only in one state. If they were to provide access to encrypted data to their home government, then not only would that government be able to access all users' data, regardless of their nationality or location, but other governments too would be able to make similar requests for access and also obtain data concerning citizens of other countries.⁴²

⁴⁰ See Kerckhoffs's principle in footnote 1.

⁴¹ When WhatsApp announced that it would change its terms of service on 8 February 2021, a poor marketing campaign led to users misunderstanding that their data would be shared with Facebook and that privacy would not be maintained. While wrong, this was enough to convince millions of users to consider switching messaging platform. In the first three weeks of January, ahead of the planned change of terms, the secure messaging apps Signal and Telegram gained 7.5 million and 25 million users respectively. See A. Hern, 'WhatsApp Loses Millions of Users after Terms Update', *Guardian*, 24 January 2021, www.theguardian.com/technology/2021/jan/24/whatsapp-loses-millions-of-users-after-terms-update.

⁴² This, among others, was an argument made by Apple when ordered by a US judge to provide access to a locked encrypted iPhone to the FBI during the investigation of the San Bernardino shooting. See Apple, 'A Message to Our Customers', 16 February 2016, www.apple.com/customer-letter/. The FBI eventually withdrew the request,

Furthermore, the hidden nature of such back-door access means that the security from outside attacks does not benefit from the same scrutiny as publicly developed solutions. This always creates the risk of attackers finding vulnerabilities introduced by the modification and using them for criminal gain. Thus, a solution that was requested to help investigations and guarantee the safety of many would instead compromise the security of all. The same risk is taken by states whose intelligence agencies compile directories of known vulnerabilities, also known as exploits, without disclosing them to manufacturers. While they may use such known vulnerabilities in secure software to access encrypted data when required (also known as ‘government hacking’), there is, first, no transparent oversight as to how and when these are used, leading to dangerous cases of ‘mission creep’, where data collection practices go beyond the initial mission statement, or other abuses of such vulnerability.⁴³ Second, there is a great risk that this knowledge will leak into the public, or at least criminal, sphere and be exploited by attackers. This is exactly what happened in May 2017 with the WannaCry ransomware attack that originated from leaked National Security Agency (NSA) exploits and affected hundreds of thousands of computer systems worldwide, including those of the United Kingdom’s National Health Service (NHS).⁴⁴

These few different aspects show that lawful access by law enforcement agencies and governments can never be achieved correctly by behind-the-scenes alternative access methods and purposefully weakened cryptographic solutions. Instead, the discussion needs to happen with the concerned public community, and it needs to move forward so that ingenious and refined technological solutions, which provide strong and specific security guarantees through transparency and established methods, can be considered. Here again Kerckhoffs’s principle would be at play: by designing a secure access technology with the assumption that its inner workings are public knowledge, it will be as strong as current research expertise can guarantee. Such a public process would furthermore help build confidence in the resulting technologies and may encourage adoption in the future.

4.4.2 *Some Potential Technological Solutions*

A few years ago, a research workshop was held in conjunction with the 2018 edition of the yearly Crypto conference with an aim to address the challenges and opportunities presented by encryption technology.⁴⁵ Regarding the specific issue of law enforcement access to encrypted data on devices, several proposals were made with the ambition to exemplify what current technology is capable of achieving and to initiate more refined discussions and research directions. It is important to point out that the following proposals do not rely on the ‘augmented’

announcing that it had found a third party that could assist it in unlocking the phone. It was later reported that this yielded no valuable information for the case. See J. Tanfani, ‘Race to Unlock San Bernardino Shooter’s iPhone Was Delayed by Poor FBI Communication, Report Finds’, *Los Angeles Times*, 27 March 2018, www.latimes.com/politics/la-na-pol-fbi-iphone-san-bernardino-20180327-story.html.

⁴³ The non-profit organisation Upturn, which aims to ‘[advance] equity and justice in the design, governance, and use of technology’, states that, in the USA, ‘[l]aw enforcement use [decryption] tools to investigate not only cases involving major harm, but also . . . graffiti, shoplifting, marijuana possession, prostitution, vandalism, car crashes, parole violations, petty theft, public intoxication, and the full gamut of drug-related offences’. See L. Koepke, E. Weil, U. Janardan, T. Dada and H. Yu, ‘Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones’, Upturn, 20 October 2020, www.upturn.org/reports/2020/mass-extraction/.

⁴⁴ D. Goodin, ‘An NSA-Derived Ransomware Worm Is Shutting Down Computers Worldwide’, *Ars Technica*, 12 May 2017, arstechnica.com/information-technology/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/.

⁴⁵ ‘Affiliated Event: Encryption and Surveillance’, Crypto 2018, 19 August 2018, crypto.iacr.org/2018/affevents/legal/page.html.

forms of encryption presented in Section 4.3; this is mainly due to the fact that these are still in the early stages of transition from academic research to software products and their full flexibility has not been explored yet, and also due to the fact that no research has been specifically aimed at using these new technologies to construct solutions for regulated access to data. That said, while the proposals that follow *are* targeted to this problem, they are also extremely novel and have not yet been either scrutinised or applied to real-world scenarios.

While these solutions may appear to provide back-door access exactly as was argued against in Section 4.4.1, they in fact differ on one important aspect: they are being proposed within a public forum. This means that important technical details can be scrutinised by numerous independent experts to ensure that the goal to secure both the content and the regulated access to that content is met. This consists in a shift of viewpoint from ‘securing data and providing occasional access’ to ‘securing data *and* occasional access’. This means that guarantees would be provided that no criminals would be able to use these solutions for illegal gain, despite knowing how the access mechanism functions. Furthermore, this creates the incentive for a new public discussion on how such an access mechanism can be regulated. The goal of this would be to establish which entities should be jointly responsible for enabling access and how abuse by corrupt regimes could be prevented.

One such solution is Matt Tait’s idea of ‘cryptographic envelopes’.⁴⁶ This proposal consists in storing on every device an encrypted version of its disk encryption key derived from the user’s secret. Importantly, the ciphertext containing the key is not created with the key itself but is instead generated with asymmetric encryption under a third party’s public key. In this way, should the third party require access to the encrypted disk, it can use its corresponding private key to decrypt the disk encryption key. One example of such a third party could be the government of the country in which the device is sold, or the device manufacturer itself, but both of these choices would leave the device vulnerable to unilateral attempts to decrypt the data. The solution proposed by Tait is to encrypt the disk encryption key with both the vendor’s and the government’s keys, thus requiring collaboration between the two organisations to enable decryption; this composition of access reduces individual risk of abuse. It could also be expanded to include other third parties’ keys, such as judicial organisations or government-independent privacy watchdogs. To link with the technology of MPC presented in Section 4.3.2, one could also imagine a solution where a single public key is used to encrypt the key but where the corresponding private key is shared between organisations within an MPC system. This would ensure that all parties would have to agree on when and what to decrypt in order for access to be granted.

As always, the risk of abuse would nonetheless remain with rogue agents attempting to subvert the regulation process or criminal organisations making targeted efforts to break the particular keys involved, and other solutions would have to be deployed to ensure that the decryptions mentioned above could not be carried out without some form of traceability and accountability. One possibility might be for organisations to keep the private keys corresponding to the public keys used by the device on hardware security modules (HSMs). These modules would be designed to record every use of the private key on tamper-proof ledgers⁴⁷ – while also recording the identity of the users making the requests – thus providing an examinable record of all decryption attempts. Should the MPC solution outlined above be used, the transcript of the MPC protocol execution could be recorded in a similar tamper-proof manner, thus preserving

⁴⁶ M. Tait, ‘Going Dark, Crypto Wars, and Cryptographic Safety-Valves’, Crypto 2018, 18 August 2018.

⁴⁷ These are digital documents which record events such as transactions or access or usage requests.

the evidence of access attempts. It would, furthermore, not leak any information regarding the private key of the system or the final disk encryption key as such MPC protocols are designed with the explicit goal that transcripts should contain no information discernible to an outsider.

Another solution presented at the aforementioned workshop is Ernie Brickell's proposal for a law enforcement access authorisation module situated directly on the device.⁴⁸ Here, during device manufacturing, an access verification key would be placed inside the device. This verification key would be the public key of an organisation that is authorised to grant access to devices. Using the corresponding private key, the organisation would create a digital signature certifying that it possesses the private key corresponding to the public key embedded into the device. With the public key, the device would then verify and approve this signature and grant one-time access to its contents. It would then be the access authorisation module's responsibility to control what could be accessed (e.g., by being technically obliged to follow a specific policy which could be set by law, such as 'contacts and messages can be accessed, but not photos'); it would therefore require a strong and secure design to ensure that it could not be modified or fooled into granting access to illegitimate parties or to unauthorised parts of the device's content. To also ensure that such a digital signature could be used to obtain access only once, it would contain a random 'number used once' (abbreviated to 'nonce') which the device could record. When presented with a new access request (in the form of a digital signature), the device would then be able to check that it had never granted access to this nonce before. This implies that, to make successive attempts at obtaining access, the party attempting it would need to repeatedly obtain new signatures from the authorising organisation.

Similar to the decryption operation in Tait's proposed solution, the generation of access-granting signatures would be strictly regulated and transparently recorded with the use of HSMs or other comparable tamper-proof recording mechanisms. Likewise, the protocol for access could be extended so that multiple signatures from independent organisations are required for access to be granted by the device. As a further measure of accountability, the device could also include a tamper-resistant user information module. This other module would be triggered when access is granted to the content of the device and, once a set amount of time has passed after access, it would inform the user by displaying the details of the access request or by altering the behaviour of the device in some way.⁴⁹ Such a solution could then be further customisable in terms of what it would grant access to, whether it would be turned out by default, whether it could be activated only for specific regions and so on.

Both proposals presented above show that modern cryptography, together with software and hardware engineering, possesses the capabilities to provide flexible, robust, transparent and accountable solutions to the issue of lawful access to encrypted devices. These and other examples (suggested at the 2018 Encryption and Surveillance workshop⁵⁰ and elsewhere) represent a welcome change in the discussion, away from the popular all-or-nothing approach. In exemplifying the security advantage and trust building that can be obtained through public consultation, they bring hope that future discussions will build on this and contribute to making the digital world a safer place for all.

⁴⁸ E. Brickell, 'A Proposal for Balancing Access and Protection Requirements from Law Enforcement, Corporations, and Individuals', *Crypto 2018*, 18 August 2018.

⁴⁹ The amount of time in question here could be set at will, either at the time of production of the device or at the time of performing the request for access.

⁵⁰ Affiliated Event, *Crypto 2018*.

4.5 CONCLUSION

In cryptographic research, the assumption that any system's design is public knowledge, and therefore available to potential adversaries, is an axiomatic principle that has driven this unprecedented development of encryption technologies over the last half a century. Naturally, the deployment of strong encryption technologies to everyday communication devices such as smartphones during the 2000s and 2010s has posed substantial challenges to law enforcement agencies when requiring access to digital evidence.

This chapter has provided a description of modern encryption technologies, from the building blocks of encryption primitives to advanced technologies, and aimed to situate them in the context of the ongoing debate on lawful access to encrypted evidence. By presenting a selection of the applications of encryption, this chapter has demonstrated that the term 'encryption' is not sufficient to encapsulate all possible challenges faced by law enforcement and that a more nuanced understanding of the variety of encryption technologies needs to be part of the debate. By then introducing more advanced technologies, such as FHE and MPC, this chapter has shown that research in cryptography is reaching a stage where data can be protected while in use (i.e., while computation is being performed), in addition to the more traditional scenarios of protection of data in transit and data at rest. While these advanced technologies are only at the beginning of their transition from research to commercial product, the last part of this chapter has presented potential technical solutions to lawful access based on more established research, demonstrating that cryptographic research principles of transparency and security can be applied to the technical challenge in question.

Recognising that access to evidence is also axiomatic to the proper functioning of a democratic justice system, this chapter has nonetheless argued that the current practice of behind-the-scenes access performed by law enforcement agencies (reinforced by the new 'decryption platform' announced by Europol) is unsustainable in the long term. Instead, this author hopes that the presentation of the burgeoning capabilities of flexible encryption can help refocus the debate on solutions where the risk is verifiably minimised.

Admissibility of Digital Evidence

Giulia Lasagni

5.1 INTRODUCTION

In the last decades, ‘digital’ or ‘electronic’ evidence has become a central element in most criminal investigations.¹ Indeed, due to the spread of informatics, today digital data is necessary to prosecute not only cybercrimes but also offences which are just incidentally committed with or facilitated by the use of some digital device.² Although the digital dimension touches upon most aspects of our daily life and simplifies many of our everyday activities, dealing with digital evidence from a legal perspective presents several complications that make the topic quite a challenging one.

To start with, the definition of digital evidence is not self-evident. In particular, it is not clear to which extent the form in which a piece of evidence is presented should be decisive in determining its legal status. In other words, it is not clear whether it is enough for information to be presented in binary form to be considered digital evidence: a typical case is a document that could otherwise be submitted in paper form. The question is relevant because – and this is a second complication to be taken into account – there is no agreement upon whether (and if so, how) rules about digital evidence should differ from the general rules of evidence, in particular when it comes to admissibility at trial.

In broader terms, the question already arises with regard to so-called forensic evidence, that is, evidence whose collection is strictly dependent on scientific expertise (e.g. DNA).³ Digital forensics, as a scientific discipline, addresses such specificities through the adoption of technical

¹ The relatively old term ‘electronic evidence’ (or ‘e-evidence’) is usually adopted in the official documents of the Council of Europe and of the European Union, and defined as ‘any evidence derived from data contained in or produced by any device, the functioning of which depends on a software program or data stored on or transmitted over a computer system or network’ (Committee of Ministers, *Guidelines on Electronic Evidence in Civil and Administrative Proceedings* (CM(2018)169-addfinal), [2019] 30 January 2019). The term ‘digital evidence’ is more recent and is usually found in international standards (on which see Section 5.3). It refers to ‘information or data, stored or transmitted in binary form that may be relied on as evidence’ (Joint Technical Committee ISO/IEC JTC 1, Information Security, Cybersecurity and Privacy Protection, ‘Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence’, ISO/IEC 27037:2012, October 2012, www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en, at 3.5). For the purpose of this contribution, the two terms will be considered as synonyms.

² See, e.g., European Commission, Commission Staff Working Document, *Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings*, SWD(2018) 118 final, 17 April 2018.

³ On which see, *ex multis*, Q. Rossy, D. Décarry-Héty, O. Delémont and M. Mulone (eds.), *The Routledge International Handbook of Forensic Intelligence and Criminology* (London: Routledge, 2017), 112 ff.; F. Schauer, ‘Can Bad Science Be Good Evidence? Neuroscience, Lie Detection and Beyond’ (2010) 95 *Cornell Law Review* 1191–1220; D. Ozonoff, ‘Epistemology in the Courtroom: A Little Knowledge Is a Dangerous Thing’ (2005) 95 *American Journal of Public*

and methodologically rigorous standards.⁴ Only seldomly, however, is compliance with the latter considered a binding requirement for the admissibility of evidence at trial in national legislation. In most cases, technical standards remain simple soft-law documents, generally applied by specialists, but devoid of any direct legal value.⁵

Within the category of forensic evidence, digital data emerges as particularly problematic. Indeed, while DNA or ballistic examinations may be relevant only for certain proceedings, digital evidence has become essential in most civil, administrative and criminal investigations; the rate is likely to increase due to the application of automated (algorithms and artificial intelligence (AI)) and robotic technologies.⁶ The need to resort to digital forensics is, therefore, increasingly looking more like the rule, rather than the exception. Hence, the renewed interest in the question of whether breaches of technical standards should have a greater impact on the admissibility of (digital) evidence.

In light of these problems, which concern legal systems at all levels, the European context emerges as especially critical. Indeed, the European Union (EU) is a single legal space in which, despite freedom of movement and circulation of goods, criminal procedure has long been defined exclusively at the national level. While this situation has slightly changed in the last few decades, rules on evidence, and admissibility of evidence in particular, remain a domain in which no clear harmonisation has been carried out yet.

Such a state of play appears highly inadequate when faced with the intrinsic transnational dimension of digital evidence. For instance, it is rather rare for service providers or cloud services to be located in the country where the information has to be retrieved and the proceedings carried out. The consequent uncertainty about the legal regime that is concretely applicable in such transnational cases, especially concerning the admissibility of evidence, negatively affects both the successful prosecution of criminal offences and the effective protection of defence and third parties' rights.

Within the EU, therefore, three questions emerge as central when touching upon the issue: Are there legal bases which support the establishment of transnational admissibility rules? Should such rules be specific to digital evidence? And, in such case, how should they be shaped?⁷

Health S13; M. F. Baumeister and D. M. Capone, 'Admissibility Standards as Politics – The Imperial Gate Closers Arrive!!!' (2003) 33 *Seton Hall Law Review* 1025; G. Gennari, 'I criteri di ammissione della prova scientifica nel contesto internazionale', in G. Canzio and L. Lupária (eds.), *Prova scientifica e processo penale* (Milan: Wolters Kluwer-Cedam, 2017), 165 ff.

⁴ More precisely, digital forensics is the discipline that applies scientific and analytical techniques to digital networks, devices and files to identify, extract, process, store and interpret digital data that could be used as evidence in (criminal, as well as other forms of) proceedings, National Institute of Justice, 'Status and Needs of Forensics Science Service Providers: A Report to Congress', 2006, www.ncjrs.gov/pdffiles1/nij/213420.pdf; see also R. Brighi, 'Una governance integrata per nuovi modelli dell'informatica forense' (2017) *i-lex. Scienze Giuridiche, Scienze Cognitive e Intelligenza Artificiale* 48–49. Several are the disciplines of digital forensics, and each requires specific expertise: Council of Europe, Cybercrime Division Directorate General of Human Rights and Rule of Law, *Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges*, Version 2.1, 6 March 2020, 134 (EEG) distinguishes computer forensics (post mortem forensics, live forensics, application forensics, Internet-of-Things forensics), mobile forensics and network forensics.

⁵ See Section 5.3.

⁶ Highlighting some of the most crucial aspects on this recent and still evolving matter, see J. L. Mnookin, 'Of Black Boxes, Instruments, and Experts: Testing the Validity of Forensic Science' (2008) 5 *Episteme* 343; S. Gless, 'AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials' (2020) 51(2) *Georgetown Journal of International Law*; G. Lasagni and G. Contissa, 'When It Is (Also) Algorithms and AI That Decide on Criminal Matters: In Search of an Effective Remedy' (2020) 28(3) *European Journal of Crime, Criminal Law and Criminal Justice* 280 ff.

⁷ Although the chapter takes a European and international perspective, references to the national dimension will be included to the extent that they are relevant in shaping a potential common way forward for the definition of digital evidence admissibility criteria.

To answer these questions, the chapter first briefly presents the main characteristics that make digital evidence so critical for the law of evidence (Section 5.2). Digital forensics standards and guidelines that describe how to collect such data, developed by the most authoritative bodies at the international and European levels, will also be illustrated (Section 5.3). Against this reconstruction, the scarce European statutory bases currently referring to the admissibility of evidence will be highlighted (Section 5.4). Given their limits, the analysis will then move to the jurisprudence of the European Court of Human Rights (ECtHR) and, especially, of the Court of Justice of the European Union (CJEU) (Section 5.5). On such grounds, some final suggestions will be exposed, supporting the need for the EU to equip itself with common admissibility criteria in general, and with specific admissibility rules concerning forensic evidence (including digital data) in particular (Section 5.6).

5.2 DIGITAL DATA: A COMMON AND FRAGILE PIECE OF EVIDENCE

Any kind of evidence can potentially be tampered with. However, the risk of alteration or deterioration is especially high in the case of digital data, which is inherently characterised by an intangible and volatile nature.⁸

Indeed, digital tracks are extremely fragile, that is to say, easily modifiable, both intentionally (e.g. by suspects who do not want to provide investigators with inculpatory information) and unintentionally. This latter case may occur through regular use (e.g. by booting up a computer) or by mishandling (e.g. by police officers lacking the necessary expertise to correctly handle a digital device at the crime scene). In some circumstances, digital data can also be easily dispersed due to the characteristics of the support storing it (e.g. if data is contained in the random access memory (RAM) of a system that gets shut down while executing some process).⁹

Although digital data might be indefinitely reproduced, contrary to analogue evidence, bits can assume a physical form only if adequately stored in a device: once altered, they cannot be restored to their previous form. In other words, from a technical standpoint, dealing with such data does not affect its authenticity, as long as appropriate procedures are complied with.¹⁰

Stressing this aspect is particularly important when it comes to the debate about the admissibility of digital evidence. In fact, especially among legal operators, digital investigations are still largely affected by so-called *data fundamentalism*, that is, the tendency to assume that analyses carried out on digital devices are *per se* reliable and objective, regardless of the adopted operational choices.¹¹ These phenomena are not unknown to other forensic sciences: for

⁸ See R. Brighi and M. Ferrazzano, 'Digital Forensics: Best Practices and Perspectives', in M. Caianiello and A. Camon (eds.), *Digital Forensic Evidence: Towards Common European Standards in Antifraud Administrative and Criminal Investigations* (Milan: Wolters Kluwer, 2021), 13 ff.

⁹ This is the case of so-called volatile data, i.e.

data that are digitally stored in a way that the probability is very high that they will be deleted, overwritten or altered within a short space of time due to human or automated interaction. Volatile data are highly fragile and will be lost if not saved quickly and correctly. In modern IT systems the amount of information held in the volatile Random Access Memory (RAM) can be as large as 16 GB or 32 GB of data (the equivalent of hundreds of thousands of pictures) and it is not just data stored in RAM that can be lost. Data in modern IT environments is not always stored and processed locally. A wide range of services offer cheap and even free storage and powerful processing resources on remote systems (i.e. the Cloud). (EEG, 67–68)

¹⁰ See ISO/IEC 27037:2012, 6 ff. The relevance of ISO/IEC standards will be illustrated in more detail in Section 5.3.

¹¹ The expression originally referred to the use of data mining techniques and automated decision-making (K. Crawford, 'The Hidden Biases in Big Data', *Harvard Business Review Blog Network*, 1 April 2013, <https://hbr.org>

instance, DNA evidence has long suffered a similar bias known as *CSI effect*, in homage to the well-known TV series.¹² Compared to other scientific domains, however, legal operators are still less accustomed to the margin of error inherent to digital investigations.¹³

Handling digital evidence, nevertheless, is a complex technical operation which requires specific expertise to be correctly performed.¹⁴ This is clearly the case in ‘digital investigations’, technically defined as the process for the ‘identification, collection, transportation, storage, analysis, interpretation, presentation, distribution, return, or destruction of digital evidence’.¹⁵ For this reason, specialised international and regional authorities have developed a series of soft-law principles and rules that should be respected when digital data is at stake.

Before moving to a more detailed analysis of said authorities, and of the problems arising from the limited legal value of their standards (Section 5.3), it is important to briefly examine some of the aforementioned technical principles: indeed, as they aim to ensure that digital data is a reliable source of information, they can become crucial also in the quest for trial admissibility criteria. To this end, three main principles will be examined here: integrity, verifiability and completeness.¹⁶

According to the principle of integrity, original data should not be altered during its acquisition, to avoid undermining *ab origine* its potential value. Obviously, the requirement does not apply only to the virtual dimension: any piece of evidence must be authentic (i.e. present itself in the same condition in which it was originally found) to be fairly used at trial. To remain in compliance with this principle, however, is especially tricky when it comes to digital data, as in this case integrity covers not only content information but also metadata. As is

[.org/2013/04/the-hidden-biases-in-big-data](http://www.oxfordjournals.org/2013/04/the-hidden-biases-in-big-data); A. Kroll, S. Barocas, E. Felten, J. R. Reidenberg, D. G. Robinson and H. Yu, ‘Accountable Algorithms’ (2016) 165 *University of Pennsylvania Law Review* 633; B. Prietl, ‘Big Data: Inequality by Design?’, Weizenbaum Conference 2019 ‘Challenges of Digital Inequality – Digital Education, Digital Work, Digital Life’, 2019, 10, www.weizenbaum-institut.de/media/Publikationen/Weizenbaum_Proceedings/Proceedings_Weizenbaum_Conference_2019.pdf) but – as a social phenomenon – it can be usefully applied in this context too.

¹² The phenomenon indicates the impact that a certain TV depiction of forensics has on judges and especially on jurors that must deal with cases involving forensic science. According to it, jurors may place a heavy emphasis on forensic science, will tend to believe that forensic evidence is 100 per cent accurate and may be reluctant to vote to convict if the prosecutor or police were unable to recover any forensic evidence from the crime scene; see S. A. Cole and R. Dioso-Villa, ‘Should Judges Worry about the CSI Effect’ (2011) 47(1–2) *Court Review* 20; M. A. Godsey and M. Alou, ‘She Blinded Me With Science: Wrongful Convictions and the Reverse CSI-Effect’ (2011) 17(4) *Texas Wesleyan Law Review* 481; J. M. Chin and L. Workewych, ‘The CSI Effect’, in M. Dubber (ed.), *Oxford Handbooks Online* (New York: Oxford University Press, 2016), 1–25.

¹³ Already in 2009 the US National Academy of Science was alerting that the ‘forensic science system exhibits serious shortcomings in capacity and quality; yet the courts continue to rely on forensic evidence without fully understanding and addressing the limitations of different forensic science disciplines’, National Research Council, National Academy of Sciences, *Strengthening Forensic Science in the United States: A Path Forward* (Washington, DC: National Academies Press, 2009), 53. While, since then, much has been accomplished with regard to certain forensics disciplines (e.g. DNA analysis has been addressed by international agreements – such as the 2005 Prüm Convention – and is the subject of several studies concerning its inherent transnational dimension – see, e.g., European Parliament, *Cross-Border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision*, June 2018, [www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU\(2018\)604971_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604971/IPOL_STU(2018)604971_EN.pdf)), when it comes digital forensics the focus is still on ‘training’ rather than on proper structural and integrated education (see, e.g., P. R. Stephenson, ‘Digital Forensic Science: An Oxymoron’ (2018) 6(2) *Legal Issues Journal* 95).

¹⁴ In the end, digital data is based on a binary system consisting of codified information (bits) that is per se not understandable by humans, unless correctly interpreted. On the relationship between ‘data’ and ‘information’, see G. Contissa, *Information Technology for the Law* (Turin: Giappichelli, 2017), 73 ff.

¹⁵ As defined in the standards Joint Technical Committee ISO/IEC JTC 1, Information Security, Cybersecurity and Privacy Protection, ‘Incident Investigation Principles and Processes’, ISO/IEC 27043:2015, March 2015; see also Section 5.3.

¹⁶ For other relevant principles in digital forensics operations, see the ISO/IEC standards, summarised also in Brighi and Ferrazzano, ‘Digital Forensics’, 16 ff.

known, metadata is essential to correctly ‘locate’ a piece of digital information in time and (virtual) space, for instance by allowing knowledge of the date of creation of a certain file, the moment in which it was downloaded, or last amended, and by which user. Such data, however, is also very easily modified when trying to access a piece of digital information. To collect integrous evidence, therefore, it is imperative that law enforcement personnel, the first to intervene at the crime scene, possess the adequate expertise to avoid unintentional alterations.¹⁷

There are, however, cases in which alteration cannot technically be avoided. This may occur, for instance, during the acquisition of data stored in the cloud or in certain smartphones.¹⁸ In these circumstances, a second principle becomes essential.

The principle of verifiability requires that each operation carried out on digital data is chronologically recorded, in what is generally called a ‘chain of custody’. The record must be such as to allow another expert, different from the one who performed the operations in the first place, to understand and potentially repeat the latter solely by looking at the chain of custody and using a copy of the data.

Hence, the chain of custody is pivotal where collecting data necessarily implies some form of alteration, as it is the only source allowing the reconstruction of the original information and the operations performed.¹⁹ Furthermore, a complete and step-by-step description of the activities carried out is always significant also from the perspective of the defendant. Examining the chain of custody can indeed allow the identification of potential mishandling or manipulation, and, therefore, challenge at trial the admissibility of the evidence so obtained.

The last fundamental principle which shall be considered in handling digital evidence is the principle of completeness. From a technical perspective, digital data makes sense – that is, it can be meaningfully attributed to a certain evidentiary value – only where acquired along with its context. In other words, the acquisition of a single file is, *per se*, meaningless. To draw credible conclusions, for instance on whether a certain piece of information (e.g. child pornography images) was intentionally stored or was the result of an automatic and involuntary download, digital forensics experts need to analyse the digital device in its entirety.

It should be said that this exigency is not exclusive to the digital domain: the need to have a complete picture of the matter under investigation does emerge also in the analogue world (e.g. the necessity to examine *all* accounting documents to understand the financial situation of a legal entity). However, a substantial difference is revealed when looking at the quality and amount of information which usually can be found in a digital device (computer, smartphone, smartwatch, smart glasses and etc.).

¹⁷ In this sense, see the technical standards illustrated in Section 5.3.

¹⁸ For instance, when conducting live data forensics, see *EEG*, 74.

¹⁹ ISO/IEC 27037:2012, § 6.1 states:

The chain of custody record is a document identifying the chronology of the movement and handling of the potential digital evidence. It should be instituted from the collection or acquisition process. This will typically be accomplished by tracing the history of the item from the time it was identified, collected or acquired by the investigating team up to the present status and location.

Among the several ways to implement chains of custody, especially relevant is the proposal to use blockchain technology, on which see H. M. Al-Khateeb, G. Epiphaniou and H. Daly, ‘Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger’, in H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou and H. Al-Khateeb (eds.), *Blockchain and Clinical Trial: Securing Patient Data*. Advanced Sciences and Technologies for Security Applications (ASTSA) (Cham: Springer International, 2019), 149–168; D. David Billard, ‘Blockchain-Based Digital Evidence Inventory’ (2019) 10(2) *Journal of Advances in Information Technology* 41–47; R. Brighi and V. Ferrari, ‘Digital evidence e tutele processuali: potenzialità della tecnologia blockchain’ (2018) 2(51) *Ragion pratica* 329 ff.

Images, videos, audios, texts (short message service, emails, notes or files), Global Positioning System (GPS) locations, internet search history, online banking information or any other record collected by various mobile applications: this data frequently dates back months, even years, allowing for pretty detailed reconstruction of different aspects of everyone's private life. In a pre-digital era, it would have been rather unlikely to find a person going around with, at the same time, photo albums, bank statements, a mapped reconstruction of their last whereabouts and a list of the topics they have lately been most interested in. Nowadays, however, 'it is the person who is not carrying a cell phone, with all that it contains, who is the exception'.²⁰ This being the context, it is clearer why digital investigation poses a difficult problem: to deliver a correct interpretation of data, technical standards recommend a complete acquisition of the information stored in the examined devices. On the other hand, a proportionate approach towards privacy and defence rights would require a careful selection of the latter, to avoid including data in the case file which is irrelevant to the proceeding or whose acquisition disproportionately affects the rights of the affected subjects (e.g. because referring only to the personal life of the defendant).²¹

The clash is significant and currently does not find an explicit solution in the European legal framework. The issue is no less critical at the domestic level either, where practices adopted by member states are still rather divergent and unconsolidated.²²

5.3 DIGITAL FORENSICS STANDARDS: AN EXPERT BUT INSUFFICIENT SOLUTION

Critical considerations, however, do not emerge only from the scattered European context, characterised by uneven legal cultures and criminal procedure legislation. Technical standards too, elaborated sometimes by private entities, sometimes by public agencies, compose sparse and occasionally overlapping methodological frameworks of procedural rules.

²⁰ As highlighted by the US Supreme Court in the landmark decision *Riley v. California*, 573 US 373 (2014), 19, mentioning also *Ontario v. Quon*, 560 US 746 (2010), 760 and Harris Interactive for Jumio, *Mobile Consumer Habits Study* (June 2013), according to which nearly three-quarters of smartphone users report being within 5 ft of their phones most of the time; 12 per cent admit they use their phones in the shower, 9 per cent during sex.

²¹ Brighi and Ferrazzano, 'Digital Forensics', 43 ff.

²² For instance, a relatively traditional solution is that of providing the defendant with the right to appoint a consultant, to assist with the selection operation; but its implementation varies across countries (e.g. in Italy and Spain the defendant has the right to appoint a (digital forensics) consultant to challenge the prosecutorial or court expert witness; in Germany the defendant is only allowed to request the court to appoint an expert witness; in Luxembourg the defendant is entitled to appoint their own consultant to attend the operations of the investigating judge's consultant, as long as this is not reckoned to delay the work of the latter).

Some states are also trying to establish more advanced forms of participated selection of digital data, though their application mostly relies on the evolution of case-law and has not found a clearly foreseeable framework yet. In Luxembourg, for instance, a participated procedure has been reportedly developed in the domestic case-law, according to which all parties (defendant and their counsellor, police and investigating judge) are to agree in advance and in writing about the procedure to be followed for the acquisition of digital data (e.g. where to keep the digital devices, which security measures to apply and so on). Though potentially very promising, the implementation of this method on a systematic basis raises several sustainability concerns, in terms of employed facilities and personnel. In Italy, the case-law is starting to consider whether mechanisms that anticipate the application of the adversarial principle also in the investigative phase (such as *accertamenti tecnici irripetibili* or *incidente probatorio*) could be applied to ensure better safeguards in the selection of digital evidence, but access to these procedures does not yet represent a clear right for the defendant. The situation is clearer in Spain, where the legislation requires that cloning of digital data shall be performed in the presence not only of the defendant but also of a third, neutral party, entrusted to guarantee the correctness of the operations carried out by the investigators (*Letrado de la Administración de Justicia*), see L. Bartoli and G. Lasagni, 'Antifraud Investigation and Digital Forensics: A Comparative Perspective', in M. Caianiello and A. Camon (eds.), *Digital Forensic Evidence: Towards Common European Standards in Antifraud Administrative and Criminal Investigations* (Milan: Wolters Kluwer, 2021), 227 ff.

The set of digital forensics guidelines which worldwide currently receives the highest recognition is that developed between 2012 and 2015 by the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC).²³ The ISO/IEC standards represent a comprehensive corpus of rules and methodologies for digital investigations, which serves as a useful reference for all cases where handling digital data is required. The guidelines thus establish technical norms which find applications in all fields of law and are not particularly drafted with criminal matters and their specificities in mind. Against such a broad scope of application, ISO/IEC standards have the merit of having identified in detail all the phases of digital investigations, illustrating for each the potential risks and necessary precautions.

In general terms, digital investigations are composed of two main steps: the acquisitive process and the investigative process. In the acquisitive phase, digital data is identified and collected from its physical location (e.g. the crime scene), to be then transported to a forensic laboratory with all due preservation and storage precautionary measures. This phase is particularly critical as usually in this context operations are carried out by so-called digital evidence first responders (DEFs), that is, individuals (like law enforcement) who should have some training in handling digital evidence, but do not have specialised expertise in the field (for instance, a degree in informatics).²⁴ It is therefore this phase which bears the highest risks of miscarriages and which could result in potential violations of the rights of the subjects involved in the investigation.

In the investigative phase, acquired data is examined, analysed and interpreted in a forensic laboratory.²⁵ These highly technical operations are performed by so-called digital evidence specialists (DES) who – unlike DEFs – are individuals characterised by specialised knowledge, skills and abilities to handle a wide range of technical issues.²⁶ They are also usually in charge of preparing a final report about the digital investigation, which translates the results of the examination into terms that are understandable also to non-informatics (e.g. the judge who has to assess the value of the digital evidence at trial).

The ISO/IEC standards are universally appreciated for their technical neutrality. This feature entails that procedural rules are drafted independently of the instruments and technologies that may be used to implement them. In other words, principles and rules are not to be dependent from the specific tools used by the investigators, which of course are continually subject to technological development and improvement.²⁷ Such an approach can therefore guarantee

²³ The ISO and the IEC are independent non-governmental international organisations committed to the development of common standards in several field matters. Relevant in regard to the topic analysed here are especially: ISO/IEC 27037:2012; Joint Technical Committee ISO/IEC JTC 1, Information Security, Cybersecurity and Privacy Protection, 'Guidance on Assuring Suitability and Adequacy of Incident Investigative Method', ISO/IEC 27041:2015, June 2015; Joint Technical Committee ISO/IEC JTC 1, Information Security, Cybersecurity and Privacy Protection, 'Guidelines for the Analysis and Interpretation of Digital Evidence', ISO/IEC 27042:2015, June 2015; ISO/IEC 27043:2015; Joint Technical Committee ISO/IEC JTC 1, Information Security, Cybersecurity and Privacy Protection, 'Electronic Discovery', ISO/IEC 27050:2019, November 2015.

²⁴ ISO/IEC 27037:2012, see also Annex A – DEFs core skills and competency definition.

²⁵ That is, laboratories specialised in handling digital exhibits and in the collection, preservation and analysis criteria they need to meet. Centralised Digital Forensics Laboratories provide investigators with the advanced tools they need for their work, making the best use of resources and skills, and bringing down the cost of forensic investigations.

²⁶ See ISO/IEC 27037:2012. In the *Guidelines on Digital Forensic Procedures for OLAF Staff*, 15 February 2016, https://anti-fraud.ec.europa.eu/document/download/87e5debi-8a64-42ca-8e08-234355dbe544_en?filename=guidelines_en_bb84583638.pdf (OLAF Guidelines), on which see s. 1.4, where DES are defined as 'OLAF staff with specialised technical expertise to perform digital forensic operations and to prepare related reports'.

²⁷ Technical neutrality has been specifically raised and tackled at the EU level by Law Enforcement Directive (Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, [2018]OJ L119, 4 May 2016, which at Recital 18 explicitly requires that

a certain stability in the investigative *modus operandi*, even in domains like informatics, characterised by rapid scientific evolution.

Against all these positive aspects, ISO/IEC standards present some significant challenges when it comes to their legal qualification. This has an impact on the rights of the parties involved in digital investigations.

First, the guidelines are not publicly accessible: being subject to copyright, they are available only upon subscription. This feature becomes critical where investigators claim to have relied on such recommendations, to support the correct performance of digital investigations. The private nature of the standards, indeed, limits the capacity of the defendant to verify the truth of such claims and reduces the foreseeability of their content.²⁸

Second, as anticipated, ISO/IEC guidelines are soft-law instruments, namely, standards devoid of any binding legal value. As they take the form of mere recommendations, their violation does not necessarily have an impact on the admissibility of the evidence collected. That is to say, interested parties (likely, the defendant) do not have a binding legal ground to invoke the inadmissibility of digital evidence, even when breaching the standards indicates that the acquired piece of evidence does not – technically speaking – retain any value.

Let's take the example of data cloning: an investigator needs to copy the data contained in a device to have it examined by forensic experts. The methodology applied to perform the cloning has a direct and pivotal impact on the potential reliability of such information: 'Copy-Paste', for instance, is not a reliable way to copy digital data, as metadata gets altered in the process.²⁹ Disregarding technical standards prevents forensic experts from interpreting such

'in order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used' (along the same line, see also Recital 15, Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, [2016] OJ L 119, 4 May 2016). On the crucial role played by this principle in digital forms of surveillance, see G. Lasagni, *Banking Supervision and Criminal Investigation: Comparing the EU and US Experiences* (Cham: Springer/Giappichelli, 2019), 349 ff.

The principle is also recognised overseas; see, for instance, Kerr, according to whom

Technology neutrality assumes that the degree of privacy the Fourth Amendment extends to the Internet should try to match the degree of privacy protection that the Fourth Amendment provides in the physical world . . . That is, the Fourth Amendment will remain technology-neutral in the sense that the overall amount and function of Fourth Amendment protection will be roughly the same regardless of whether a wrongdoer commits his crime entirely online, entirely in the physical world, or using a mix of the two. (O. S. Kerr, 'Applying the Fourth Amendment to the Internet: A General Approach' (2010) 62(4) *Stanford Law Review* 1015 ff)

²⁸ This issue has been identified as problematic by the ECtHR, although in cases not directly related to digital investigations, in light of the proportionality principle. See *Zakharov v. Russia*, Appl. no. 47143/06, 4 December 2015, § 241 ff, where the publication of technical requirements in a magazine distributed only through subscription was critically considered by the Court (although the most emphasis concerning legal bases was posed on the requirements of 'foreseeability' and 'necessity', which were especially critical in the case at stake):

The Court accepts that the addendums to Order no. 70 mainly describe the technical requirements for the interception equipment to be installed by communications service providers. At the same time . . . the addendums to Order no. 70 are capable of affecting the users' right to respect for their private life and correspondence. The Court therefore considers that they must be accessible to the public.

²⁹ Reliable techniques are instead, for instance, those referring to the so-called bit-stream image, i.e. cloning of a memory duplicating each bit according to the order in which it is found in the original; if correctly performed, the copy will be identical to the matrix, and their correspondence can be verified; see, e.g., E. Casey, *Digital Evidence and Computer Crime*, 3rd ed. (Amsterdam: Academic Press, 2011), 22 ff. In order to verify that a file has not changed during, e.g., an acquisition from a device, or to find copies of known contraband, also mathematical techniques that compute a hash value, can be used; see, e.g., J. R. Lyle, B. Guttman, J. M. Butler, K. Sauerwein, C. Reed and C. E. Lloyd, *Digital Investigation Techniques: A NIST Scientific Foundation Review*, US Department of Commerce NISTIR 8354-DRAFT (Gaithersburg, MD: National Institute of Standards and Technology, May 2022).

data, and from assigning it a meaningful value to which legal consequences could be attached (e.g. by stating that the data was intentionally stored in the device by the accused). However, because technical standards do not have a legally binding value, nothing in principle prevents legal operators, and judges in particular, from considering the same data admissible at trial.

The issue is particularly acute in the EU where, due to the lack of common statutory rules on the admissibility of evidence, the matter relies entirely on national regimes and European case-law, with rather ambiguous results. As will be further illustrated, indeed, the first are rather diverging and generally poorly foreseeable in the transnational context (anything but rare when it comes to digital data, see Section 5.4). On the other hand, the latter has only recently started to take a more decisive stand on the matter and, though promising, is still far from having established clearly settled criteria (Section 5.5).

The picture is then further complicated by the fact that, taking the ISO/IEC principles and rules as a model, numerous national and European authorities have developed their own set of standards for digital forensic investigations, giving rise to a multiform framework of soft-law instruments.³⁰ Nonetheless, some shared principles and rules seem to emerge that can provide interesting insights into what common rules on the admissibility of digital evidence should look like. Given the focus of the analysis, the following paragraphs will mainly deal with standards elaborated by the Council of Europe and the EU, while reference to national guidelines will be made only to the extent necessary to highlight significant divergences.

5.3.1 Digital Forensics Standards: The Council of Europe

Among the guidelines developed by the Council of Europe, there are two documents of major interest. The first set of standards is the *Electronic Evidence Guide. A Basic Guide for Police Officers, Prosecutors and Judges* (EEG), initially issued in 2013. The EEG has a specific focus on digital investigations in the criminal law domain, as it addresses law enforcement and judicial authorities. Its goal is to help them acquire basic technical knowledge on what digital information and devices are, as well as to present the best practices to correctly handle digital traces on a crime scene.³¹

The EEG is intended to be used as a starting point for domestic legislators, to elaborate detailed standards which also take into account the relevant national law on evidence. Thus, the document does not explicitly contain detailed provisions concerning typically criminal procedure profiles, such as rules on the admissibility of evidence. However, some positioning relevant to the matter can be found in the document.

³⁰ This is the case, for instance, of Spain, where specific standards have been developed which – like ISO/IEC – are not publicly accessible, though applied by the *policía científica* (see UNE – *Una Norma Española*, as illustrated by L. Bachmaier Winter, ‘The Handling of Digital Evidence in Spain’, in M. Caianiello and A. Camon (eds.), *Digital Forensic Evidence* (Milan: Wolters Kluwer, 2021) 169 ff.). In Germany, *IT-Forensik* guidelines have been developed at the federal level, but further standards are then developed at the state level by single authorities (see S. Gless and T. Wahl, ‘The Handling of Digital Evidence in Germany’, in M. Caianiello and A. Camon (eds.), *Digital Forensic Evidence* (Milan: Wolters Kluwer, 2021), 64 ff.); in Italy, digital forensics guidelines have been drafted in the form of internal Circulars of the financial police (*Guardia di Finanza*), not all publicly available and with a limited scope of application, i.e. for antifraud investigations (Comando generale della Guardia di Finanza, III Reparto Operazioni – Ufficio Tutela Entrate, ‘Manuale operativo in materia di contrasto all’evasione e alle frodi fiscali’, Circolare no. 1/2018, Vol. II (Part III: ‘Esecuzione delle verifiche e dei controlli’, ch. 2, ‘Poteri esercitabili’), see L. Bartoli and G. Lasagni, ‘The Handling of Digital Evidence in Germany’, in M. Caianiello and A. Camon (eds.), *Digital Forensic Evidence* (Milan: Wolters Kluwer, 2021), 89 ff.). Particularly authoritative, also at the international level, are then the British standards: DAC Janet Williams QPM, ‘ACPO Good Practice Guide for Digital Evidence’, March 2012, www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.

³¹ ISO/IEC 27037:2012.

For one, the *EEG* stresses the need for a link between compliance with the best technical standards and the admissibility of digital evidence. The fact that digital ‘evidence is admissible if it conforms to a series of laws and rules that ensure it is acceptable to the court’ and that ‘proper [technical] procedures must be followed when obtaining evidence’³² is actually a very significant statement. This is even more so, considering the emphasis put by the *EEG* on the fact that ‘the onus is on the prosecution to show to the court that the evidence produced is no more and no less now than when it was first taken into the possession of law enforcement’.³³ Thus, the *EEG* recommendations seem to support a system in which the exclusion of evidence could be invoked, when digital evidence is collected in violation of the technical standards agreed upon by the relevant scientific community.

Nonetheless, this approach does not always find a coherent application throughout the whole guide. For instance, on the one hand the *EEG* advocates that, in criminal proceedings, ‘electronic evidence is subject to the same rules and laws that apply to documentary evidence’: both need to be authentic, their only difference being ‘the ease with which electronic evidence can be changed and altered, either deliberately or inadvertently’.³⁴ Arguably, the rationale behind such a linear equivalence may be open to criticism: it could be reckoned that precisely because of their diverse degree of vulnerability, the admissibility of digital evidence should be subject to further and more safeguarding criteria than those concerning documentary evidence. On the other hand, the same *EEG*, elsewhere, seems to support this understanding in line with its recommendations. For example, the provisions to ‘use standardised forms or checklists to document’ the operations of digital forensics³⁵ and to ‘record the search and seizure by video’³⁶ seem to set rules that are specific to e-evidence only.³⁷

The second significant set of standards developed by the Council of Europe on the matter of digital investigation is the *Guidelines on Electronic Evidence in Civil and Administrative Proceedings* (henceforth: the *Guidelines*).³⁸ Although not directly addressing criminal investigations, these standards show an approach interesting also to the latter.

The *Guidelines* tackle the existence of ‘obstacles to the effective management of electronic evidence within justice systems, such as the lack of common standards and the diversity and complexity of evidence-taking procedures’, inviting states to ‘examine current deficiencies in the use of electronic evidence and to identify the areas where electronic evidence principles and practices could be introduced or improved’.³⁹ More specifically, the *Guidelines* voice some

³² See *EEG*, § 7.2.1 (at 151); see also § 9.2.4 (at 159), where it is also affirmed in general terms that digital evidence in criminal trial ‘must be admissible, authentic, accurate and complete. It must conform to applicable laws and rules and be acceptable to the court.’

³³ See *EEG*, § 7.3 (at 152).

³⁴ See *EEG*, §§ 7.3 (at 152) and 7.2.2 (at 151).

³⁵ See *EEG*, at 138.

³⁶ See *EEG*, § 7.1 (at 151). Recording where the digital device was found and seized is important

because it can reveal a great deal about the intent of the suspected offender. It is good practice to record the search and seizure by video. This will show the position of digital devices, so that there is no longer an argument, for instance, as to whether the wireless device was found hidden in the loft rather than in an open access area in the sitting room.

³⁷ Similarly relevant appears also the recommendation to ‘consider if it is necessary and/or desirable to inform the owner or user of the identified electronic device that the capture process that will take place, or if whether the procedure can be ex parte’, *EEG*, at 163.

³⁸ Council of Europe, *Guidelines on Electronic Evidence in Civil and Administrative Proceedings*, CM(2018)169-addfinal, 30 January 2019 (*Guidelines*).

³⁹ See the preamble of the *Guidelines*.

recommendations already included in the ISO/IEC standards, for instance concerning the essential need to provide adequate training and education for all actors involved in judicial proceedings (judicial authorities, law enforcement, lawyers, third parties)⁴⁰ on how to preserve electronic data,⁴¹ and on the relevance of metadata to the probative value of digital information.⁴²

Moreover, the *Guidelines* explicitly refer to three ‘fundamental principles’, used during the (civil) trial of digital evidence, that are also rather relevant for the analysis at stake. The first principle affirms that the ‘potential probative value’ of such data be established ‘in accordance with national law’.⁴³ Although expressed in very general terms, the need to establish a clear legal basis for the admissibility of digital evidence indeed represents a substantial development to the current legal framework, especially at the supranational level.

The second ‘fundamental principle’ contained in the *Guidelines* states that ‘electronic evidence should be evaluated in the same way as other types of evidence, in particular regarding its admissibility, authenticity, accuracy and integrity’. This provision is also relevant as it addresses the risk of a ‘diminished’ use of digital evidence, in favour of other kinds of (physical) evidence judges may be more accustomed to. Furthermore, recalling the general principles explained as regards the ISO/IEC standards, they underline the importance of relying at trial only on e-evidence characterised by a certain intrinsic ‘quality’.

The third and last principle is perhaps the most interesting, particularly from the point of view of the defence as it connects the adoption of adequate standards in handling digital evidence with the notion of procedural fairness.⁴⁴ Although rather generic in its formulation, the principle shows paramount importance at the European level, where rules on (digital) evidence admissibility are still quite deficient, but the notion of fair trial is instead rather developed. Especially in criminal law, the possibility to consider breaches of technical standards as fair trial violations could indeed open significant perspectives for the parties involved in digital investigations. This

⁴⁰ See *Guidelines*, §§ 31–35 and § 12. According to § 32, in particular, ‘Member States should keep technical standards related to electronic evidence under review’. States should also ‘promote awareness of the benefits and value of electronic evidence’, so that judges and legal practitioners are made aware ‘of the specific issues that arise when dealing with the seizure and collection of electronic evidence abroad, including in cross-border cases’ (§ 12), and ‘of the evolution of information technologies which may affect the availability and value of electronic evidence’ (§ 34). Multidisciplinary education for all professionals dealing with electronic evidence is then required, explicitly stating that ‘legal education should include modules on electronic evidence’ (§ 35).

⁴¹ *Guidelines*, §§ 25–30, requiring to establish appropriate manners so as to preserve, also ‘over time, taking into account the evolution of information technology’, the ‘readability, accessibility, integrity, authenticity, reliability and, where applicable, confidentiality and privacy’. In order to achieve this, the archiving of electronic data should be carried out by qualified specialists (§ 29).

⁴² *Guidelines*, § 8: Courts should ‘be aware of the probative value of metadata and of the potential consequences of not using it’. The importance of metadata as a necessary element to correctly assess digital evidence is also reaffirmed at § 26, where it is stated that, to make clear which is the ‘context of its creation’, electronic evidence should be stored ‘with standardised metadata’.

⁴³ The approach is confirmed in the preamble, which clearly states that the *Guidelines* should not be ‘interpreted as prescribing a specific probative value for certain types of electronic evidence and are to be applied only insofar as they are not in conflict with national legislation’. If ‘complex evidentiary issues are raised’ or ‘manipulation of electronic evidence is alleged’, courts are recommended to ask for the support of an expert in order to clarify the technical profiles included in the assessment. Ultimately, however, according to the *Guidelines*, the decision on the reliability of digital evidence shall be in the hands of the judge, and of the judge alone (§ 18). Courts should also be able to ‘decide whether such persons have sufficient expertise in the matter’; in assessing the ‘source and authenticity’ of electronic evidence, ‘all relevant factors should be considered’ (§ 29).

⁴⁴ ‘The treatment of electronic evidence should not be disadvantageous to the parties or give unfair advantage to one of them.’ And actually the collection of digital evidence should be performed in ‘an appropriate and secure manner’, having regard to ‘the higher risk of the potential destruction or loss ... compared to non-electronic evidence’ (§§ 10–11).

potential is even more interesting in light of the standards developed within the EU in matters of digital forensics.

5.3.2 Digital Forensics Standards in the European Union

Digital forensics standards developed in the context of the EU show specific attention to the bond between technical reliability and procedural fairness. The two main important documents in this domain are the 2015 European Union Agency for Cybersecurity (ENISA)'s *A Basic Guide for First Responders (Basic Guide)* and the 2016 *Guidelines on Digital Forensic Procedures for OLAF Staff (OLAF Guidelines)*.⁴⁵

The *Basic Guide* provides a detailed set of guidelines for digital investigations, with a specific focus on cybersecurity.⁴⁶ Similarly to the *EEG*, this document does not aim at creating an autonomous corpus of digital forensic standards; furthermore, it does not exclusively refer to criminal investigations. However, its specific focus sheds a light which opens an interesting perspective on the admissibility issue examined in this chapter.

As revealed by its name, the *Basic Guide* focuses on the first steps (acquisitive process) of digital investigations, which fall under the competence of first responders.⁴⁷ As illustrated earlier, this is a delicate phase of the procedure in which the intervening law enforcement personnel usually do not have specific expertise in informatics; thus, it is where violations of technical standards are more likely to occur.

The *Basic Guide* aims at filling this gap by providing dedicated training and ensuring a basic qualification that could also be formalised with a certification system. The underlying idea is that such personnel should receive dedicated training, which – though not making them informatics specialists – enables law enforcement to carry out the first steps of digital investigation in a technically proper way. To this end, the *Basic Guide* lists a series of requirements that investigators need to comply with, when approaching a digital device. For instance, the document indicates that first responders' activity should be not only recorded in writing but also video-recorded 'in order to create accurate depictions of the scene'.⁴⁸

⁴⁵ Another relevant document in the field is European Network of Forensic Science Institutes (ENFSI), *Best Practice Manual for the Forensic Examination of Digital Technology. Version 01*, November 2015, https://enfsi.eu/wp-content/uploads/2016/09/1_forensic_examination_of_digital_technology_o.pdf. Established in 1995, the ENFSI includes today thirty-eight European countries, including all EU member states except Luxembourg. The purpose of the ENFSI as a network of experts is to share knowledge, exchange experiences and come to mutual agreements in the field of forensic science, including the domain of digital evidence. To achieve this, the ENFSI in particular encourages all the laboratories that are part of the network to comply with best practice and international standards for quality and competence assurance. Against this background, the *Manual* is mainly focused on the implementation in forensic laboratories of the requirements of international and local regulatory standards.

⁴⁶ European Union Agency for Cybersecurity (ENISA), 'Electronic Evidence – A Basic Guide for First Responders', March 2015, www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders. Under the name European Network and Information Security Agency, ENISA was established by Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, [2004] OJ L 77, 13 March 2004, and is currently regulated by Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act), [2019] OJ L 151, 7 June 2019. In the same time period, it also issued ENISA, *Digital Forensics: Handbook, Document for Teachers*, September 2013, www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/documents/digital-forensics-handbook, aiming at supporting teachers who need to structure training courses on digital forensics and evidence gathering for personnel involved in the process of early fraud investigations.

⁴⁷ See Section 5.3.

⁴⁸ See ENISA, 'Electronic Evidence – A Basic Guide for First Responders', respectively at 17 and 14.

Reading such parameters in light of the law of evidence, several questions could accordingly be raised that directly touch upon the rules on admissibility. For instance: should a piece of digital information be declared inadmissible if collected by law enforcement personnel that do not possess a basic qualification, or that did not follow technical standards when performing digital forensic operations (e.g. by not video-recording the activities performed on the device)? In other words, the issue arises as to whether the breach of technical rules should be invoked by the accused, to sustain the inadmissibility of the collected evidence.

A tentative step further towards the ‘proceduralisation’ of technical rules can be observed in the *OLAF Guidelines* developed by the European Anti-Fraud Office.⁴⁹ Although limited in its scope in combating fraud against EU financial interests, OLAF standards are very significant, especially from the perspective of the defendant: these guidelines indeed provide for a series of information and participation rights which resemble more closely provisions usually found in criminal procedure codes and legislation than mere soft-law recommendations.

With regard to first responders, for instance, the *OLAF Guidelines* require that only expert personnel shall be entitled to ‘accept digital devices from persons during the digital forensic operation’, while investigators not qualified in that respect shall refrain from doing so.⁵⁰ In other words, during OLAF investigation, personnel who do not possess at least a basic digital forensics knowledge cannot be employed even for very basic (but potentially decisive) activities, such as acquisition of the device.

Furthermore, when performing digital investigation, OLAF staff are required to hand the person or the economic operator subject to the operation a copy of the *Digital Forensic Operations Information Leaflet*, which provides information on the procedural safeguards that the investigators shall comply with, in particular, in light of the ‘principles of legitimacy, necessity, and proportionality’.⁵¹

For instance, the *OLAF Guidelines* recognise the right of the person from which data has been collected to be informed of the maximum amount of time for which it can be retained by the authorities. Despite the provision of a very long term (fifteen years after the closure of the investigation),⁵² fixing a deadline after which the seized data cannot be retained any longer shows an awareness of the rights of the subjects involved that is rarely addressed by other relevant standards.

Furthermore, a specific provision acknowledges the problems arising from the principle of completeness during data acquisition.⁵³ Accordingly, in the first phase, ‘OLAF investigators are empowered to assume custody or forensically acquire data . . . even if they contain personal data which are not relevant’. However, ‘access and further process’ of the information so collected is limited only to that ‘relevant to the investigation’.⁵⁴ Hence, OLAF standards allow investigators to gather all available data, but an intermediary selection phase shall occur to filter what can actually be used for investigative purposes. Neither the *OLAF Guidelines* nor the *Leaflet* provides a detailed

⁴⁹ *OLAF Guidelines*. The European Anti-Fraud Office (OLAF, from the French: Office européen de lutte antifraude) is the independent office in charge of carrying out administrative investigations concerning fraud against the EU budget, corruption and serious misconduct within the European institutions, and of developing anti-fraud policy for the European Commission.

⁵⁰ Contrary to ISO/IEC standards, the *OLAF Guidelines* do not explicitly define ‘first responders’, but they can nonetheless be identified by exclusion from the definition of digital evidence specialist (DES): ‘OLAF staff with specialised technical expertise to perform digital forensic operations and to prepare related reports’ (§ 1.4).

⁵¹ See *OLAF Guidelines*, § 4.2. European Anti-Fraud Office, *OLAF Digital Forensic Operations Information Leaflet*, https://anti-fraud.ec.europa.eu/system/files/2021-09/digital_forensic_leaflet_en.pdf (*OLAF Leaflet*).

⁵² See *OLAF Leaflet*, sub ‘What will OLAF do with the data which have been acquired/collected?’.

⁵³ See Section 5.2.

⁵⁴ See *OLAF Leaflet*, ‘What if my digital device contains personal data not relevant to the investigation?’.

reconstruction of how the selection mechanism actually works in practice (e.g. Who selects the relevant data? Can the investigated subject have a say in the process? Is there any remedy to quash the decision of the investigators?). Nonetheless, the idea of a specific selection phase following the acquisition of the data also represents an interesting step forward in addressing an issue crucial in digital investigations, upon which admissibility of evidence is strictly connected.

5.4 ADMISSIBILITY OF (DIGITAL) EVIDENCE IN EUROPEAN LEGISLATION: AN UNCERTAIN STATE OF PLAY

As anticipated, against the proliferation of soft-law instruments on digital forensics, in Europe no harmonised rules exist at the statutory level that regulate how digital evidence ought to be collected in order to be admissible at trial.⁵⁵ The issue, worth reminding, does not concern the digital sphere exclusively: regardless of its electronic or physical nature, to date evidence law in general and admissibility rules in particular remain a field in which the European supranational framework is highly deficient.⁵⁶ To a certain extent, such an image may come as a surprise when looked at from the angle of digital evidence: for once, the Council of Europe has historically been one of the greatest international propulsors in developing common standards on the increasing technological dimension of criminal law and investigations.⁵⁷

The 2001 Budapest Convention, especially, has been recognised as a worldwide reference for the fight against cybercrime, and, mostly thanks to its technical neutrality, still retains the title more than twenty years after its approval.⁵⁸ The treaty notably established the first harmonised rules on digital investigations, requiring state parties to make available in their legislation both the necessary investigative techniques⁵⁹ and the necessary

⁵⁵ The recent 2023 Proposal for a Directive on Mutual Admissibility of Evidence and E-Evidence in Criminal Proceedings, formulated by the European Law Institute (ELI), represents a step forward in this direction, although just at the level of academic proposal. See www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf; and, for a first assessment of the proposal, see L. Bachmaier Winter and F. Salimi (eds.), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights* (Oxford: Hart, 2024).

⁵⁶ So it has to be called ‘one of the great taboos’ of the European criminal justice, see J. A. E. Vervaele, ‘Lawful and Fair Use of Evidence from a European Human Rights Perspective’, in F. Giuffrida and K. Ligeti (eds.), *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings* (Luxembourg: University of Luxembourg Press, 2019), 62, highlighting that the theme ‘has been greatly neglected by all cooperation instruments, be they instruments of mutual legal assistance or mutual recognition’.

⁵⁷ See, most recently, also with regard to automated technology, e.g., European Commission for the Efficiency of Justice (CEPEJ), *European Ethical Charter on the Use of Artificial Intelligence (AI) in Judicial Systems and Their Environment*, 3–4 December 2018, <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>.

⁵⁸ Council of Europe, *Convention on Cybercrime*, ETS No. 185, 23 November 2001, on which see M. A. Vatis, ‘The Council of Europe Convention on Cybercrime’, in National Research Council, *Proceedings of a Workshop on Detering Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, DC: National Academies Press, 2010), 207 ff; M. Gercke, ‘10 Years Convention on Cybercrime’ (2011) 12(5) *Computer Law Review International* 142 ff; P. de Hert, C. Parlar and J. Sajfert, ‘The Cybercrime Convention Committee’s 2017 Guidance Note on Production Orders: Unilateralist Transborder Access to Electronic Evidence Promoted via Soft Law’ (2018) 34(2) *Computer Law & Security Review* 327 ff.

⁵⁹ Production orders, search, real-time collection of traffic data and interception of content data (Arts. 18–21). According to Article 20, a competent authority shall also be able to collect or record through the application of technical means on its territory or to compel a service provider, within its existing technical capability, to (a) collect or record or (b) co-operate and assist the competent authority in the collection or recording of traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. Where such real-time monitoring systems are not allowed at the national level due to ‘established principles of its domestic legal system’,

powers⁶⁰ to effectively carry them out. The Convention requires that investigative measures be implemented subject to the conditions and safeguards recognised by national law. State parties, however, do not enjoy unlimited discretion on the matter, as they must provide for adequate protection of human rights and liberties and incorporate the principle of proportionality. More specifically, the treaty requires national legislation to (at least) establish which grounds may justify application of such measures, to limit their scope and duration and, in any case, to recognise the right to a judicial review (or to a remedy before an independent authority).

Hence, the Convention demands that digital investigative measures be carefully drafted in national law, shaping their scope of application and legal conditions, in light of the impact that the underlying technologies may produce on the fundamental rights of the accused. In other words: digital investigations, likely much more pervasive than their physical correspondents (e.g. in case of searches), need to find a legal basis in national systems, and one with adequate quality requirements that take into account the degree of intrusiveness of the measures at stake.⁶¹

For what concerns the topic of this chapter, however, no specific provision can be found in the Budapest Convention that explicitly deals with the admissibility of evidence. The treaty, for instance, does not state whether legal bases should be specifically drafted for the digital dimension of the investigations or whether an analogue application of more general rules could suffice. States parties then opted for different solutions, in some cases by introducing *ex novo* legislation to regulate the phenomena,⁶² in other cases by broadening the scope of application of pre-digital pieces of legislation to include also the new digital dimension.⁶³ This scattered implementation has resulted in a supranational framework where, at best, regulation of the same investigative measures diverges greatly at the European level and, in the case where transnational investigative measures are performed, reduces the clarity and foreseeability of the relevant legal basis.

The picture is not much different when looking at the EU legal framework. As such, criminal procedure is not the most developed field of Union law, despite a definite increase in the last few decades.⁶⁴ The EU is, however, steadily showing a direct interest in fighting the digital dimension of criminality and empowering transnational criminal prosecution tools capable of doing

a state may instead adopt legislative and other measures to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. For a recollection of the investigative technique applied in banking investigations, see Lasagni, *Banking Supervision and Criminal Investigations*, 300 ff.

⁶⁰ To seize and secure data, make and retain a copy, store data and compel informatics experts to cooperate, see Article 19 of the Budapest Convention.

⁶¹ See *Zakharov v. Russia*, § 228.

⁶² As it is, for instance, in the case of Spain, which introduced a whole new set of legal provisions concerning a good part of digital investigative measures (Art. 588 *sexies* and ff of the Criminal Procedure Code, as amended by the Organic Law 13/2015, on which see in detail Bachmaier Winter, 'The Handling of Digital Evidence in Spain', 175 ff.).

⁶³ As it is, for instance, in the cases of Belgium and France (on which see V. Franssen and O. Leroux, 'Recherche policière et judiciaire sur internet : analyse critique du nouveau cadre législatif belge', in V. Franssen and D. Flore (eds.), *Société numérique et droit pénal. Belgique, France, Europe* (Brussels: Larcier/Bruylant, 2019), 135–216) or Italy (on which see L. Cuomo, 'La prova digitale', in G. Canzio and L. Lupária (eds.), *Prova scientifica e processo penale* (Milan: Wolters Kluwer-Cedam, 2017), 669 ff.).

⁶⁴ Thanks to the implementation of the so-called Stockholm Programme (Council of the European Union, *The Stockholm Programme – An Open and Secure Europe Serving and Protecting the Citizens*, No. 17024/09, 2 December 2009), six Directives were approved on procedural safeguards in criminal proceedings focused on the defendant (Directive 2010/64/EU of 20 October 2010 on the right to interpretation and translation in criminal proceedings, [2010] OJ L 280, 26 October 2010; Directive 2012/13/EU of 22 May 2012 on the right to information in criminal proceedings, [2012] OJ L 142, 1 June 2012; Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, [2013] OJ L 294, 6 November 2013; Directive

so. Tangible examples in this sense may be found, for instance, looking at the Anti-Money Laundering/Countering the Financing of Terrorism legislation,⁶⁵ which has been extended in order to include also virtual assets and fintech,⁶⁶ or at the recently operational European Public Prosecutor Office.⁶⁷ Though still very recent, and thus more difficult to assess, similar considerations apply even more to the Artificial Intelligence Act⁶⁸ or to the new cooperation tool specific to digital evidence (the European Production Order).⁶⁹

(EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, [2016] OJ L 65, 11 March 2016; Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings, [2016] OJ L 132, 21 May 2016; Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings, [2016] OJ L 297, 4 November 2016) and one was approved on victims' rights (Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, [2012] OJ L 315, 14 November 2012).

⁶⁵ Terrorist financing and money laundering have been made explicitly prosecutable when referring to 'assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital'; for the definition of 'funds' and 'property', see, respectively, Article 2(1), Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, [2017] OJ L 88, 31 March 2017, and Article 2(2), Directive (EU) 2018/1673 of 23 October 2018 on combating money laundering by criminal law, [2018] OJ L 284, 12 November 2018. Directive 2017/541 on combating terrorism explicitly praises the need for strong coordinated cooperation 'with a view to securing and obtaining electronic evidence' (Recital 7).

See also Article 1(1)(c), let. (g) and (h), Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, [2018] OJ L 156, 19 June 2018, which included in the list of undertakings subject to the AML/CFT reporting regime also providers engaged in exchange services between virtual currencies and fiat currencies, and custodian wallet providers.

⁶⁶ Other examples may be found in Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, [2011] OJ L 335, 17 December 2011; Directive 2013/40/EU of 12 August 2013 on attacks against information systems, [2013] OJ L 218, 14 August 2013; and, more recently, Directive (EU) 2019/713 of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment, [2019] OJ L 123, 10 May 2019, and Regulation (EU) 2020/493 of the European Parliament and of the Council of 30 March 2020 on the False and Authentic Documents Online (FADO) system and repealing Council Joint Action 98/700/JHA, [2020] OJ L 107, 6 April 2020.

⁶⁷ Although the EPPO competence, for the time being, is limited only to financial crimes (Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), [2017] OJ L 283, 31 October 2017), proposals have already been submitted to extend its scope of action, see Communication from the Commission to the European Parliament and the European Council, *A Europe That Protects: An Initiative to Extend the Competences of the European Public Prosecutor's Office to Cross-Border Terrorist Crimes* (COM(2018)641 final), [2018], 12 September 2018.

⁶⁸ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, on which see critically, *ex multis*, Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22(4) *Computer Law Review International* 97–112; M. Ebers, 'Truly Risk-Based Regulation of Artificial Intelligence – How to Implement the EU's AI Act' (19 June 2024), <http://dx.doi.org/10.2139/ssrn.4870387>.

⁶⁹ When this new tool enters into force, it will deal with digital evidence but only to regulate the cooperation mechanism to acquire it from service providers, without providing for common rules establishing how digital investigations should be carried out, see Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings and Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, on which see V. Franssen, 'The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?', *European*

Nonetheless, within the criminal justice domain, very few pieces of legislation touch upon evidence law, and none with a clear harmonising intent. In particular, the Directive on the European Investigation Order⁷⁰ and the Regulation on freezing and confiscation orders⁷¹ deal with the topic from the perspective of ensuring mutual recognition, that is, facilitating enforcement of investigative, seizure, freezing or confiscation measures throughout the EU. Hence, at least explicitly, these texts do not prescribe common conditions or requirements that should be met when investigative measures are applied.⁷² This state of play has been repeatedly stressed as critical, and potentially capable of impairing the effectiveness of integration carried out so far in criminal matters.⁷³

Law Blog, 12 October 2018, <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN>; see also Chapter 7 in this volume.

⁷⁰ Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, [2014] OJ L 130, 1 May 2014. Among the extensive literature on the matter, see, *ex multis*, S. Tosza, 'All Evidence Is Equal, but Electronic Evidence Is More Equal Than Any Other: The Relationship between the European Investigation Order and the European Production Order' (2020) 11(2) *New Journal of European Criminal Law* 161 ff.; I. Armada, 'The European Investigation Order and the Lack of European Standards for Gathering Evidence: Is a Fundamental Rights-Based Refusal the Solution?' (2015) 6(1) *New Journal of European Criminal Law* 8; S. Allegrezza, 'Collecting criminal evidence Across the European Union: The European Investigation Order between Flexibility and Proportionality', in S. Ruggeri (ed.), *Transnational Evidence in Multicultural Inquiries in Europe Developments in EU Legislation and New Challenges for Human Rights-Oriented Criminal Investigations in Cross-Border Cases* (Heidelberg: Springer, 2014), 51–67; C. Heard, 'The European Investigation Order: Changing the Face of Evidence-Gathering in EU Cross-Border Cases' (2011) 2(4) *New Journal of European Criminal Law* 353–367; L. Bachmaier Winter, 'European Investigation Order for Obtaining Evidence in the Criminal Proceedings Study of the Proposal for a European Directive' (2010) 9 *Zeitschrift für Internationale Strafrechtsdogmatik* 580.

⁷¹ Regulation (EU) 2018/1805 of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders, [2018] OJ L 303, 28 November 2018. On this increasingly emerging field of EU cooperation, see, e.g., A. Bernardi (ed.) and F. Rossi (coord.), *Improving Confiscation Procedures in the European Union* (Naples: Jovene, 2019).

⁷² With the exception of Article 31 of the EIO Directive, which specifies rules in relation to findings involving interception of telecommunication carried out without technical assistance of the notified member states: these 'may not be used, or may only be used under conditions which it shall specify, in case where the interception would not be authorised in a similar domestic case', as highlighted by K. Ligeti, B. Garamvölgyi, A. Ondrejová and M. von Galen, 'Admissibility of Evidence in Criminal Proceedings in the EU' (2020) 3 *Eu crim* 202.

⁷³ See, e.g., the Commission services preliminary views following the consultations on the European Production Order, which in 2017 underlined the need for common 'EU criteria' to address the cross-border dimension of digital investigations, which do not strictly concern only cooperation but can also 'provide conditions to be fulfilled for certain investigative measures', Council of the European Union, *Technical Document: Measures to Improve Cross-Border Access to Electronic Evidence for criminal investigations Following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace*, No. 9543/17, 6, www.consilium.europa.eu/en/documents-publications/public-register/public-register-search/results/?AllLanguagesSearch=False&OnlyPublicDocuments=False&DocumentLanguage=EN&ImmIdIdentifier=ST%209554%202017%20INIT. Also the European Parliament highlighted the 'difficult access to e-evidence, problems in obtaining it and with its admissibility in court', stressing 'the need to develop shared procedural standards . . . and to define investigative measures which can be used regardless of geographic borders', European Parliament, *Resolution of 3 October 2017 on the Fight Against Cybercrime* (2017/2068(INI)), 3 October 2017, Recital M, §§ 59, 66, 67. The need to adopt common admissibility rules emerged already in Commission of the European Communities, *Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility* (COM/2009/0624 final), 11 November 2009, 5.2 ('6. Would you in principle welcome the introduction of common standards for gathering evidence? Why? 7. Would you prefer to adopt general standards applying to all types of evidence or to adopt more specific standards accommodated to the different types of evidence? Why?'). The magnitude of the problems arising from this lacuna is stressed also by the literature, see, *ex multis*, Vervaele, 'Lawful and Fair Use of Evidence', 56 ff.; G. Vermeulen, W. De Bondt and Y. Van Damme, *EU Cross-Border Gathering and Use of Evidence in Criminal Matters. Towards Mutual Recognition of Investigative Measures and Free Movement of Evidence?* (Antwerp: Maklu, 2010), 145 ff.; K. Ligeti (ed.), *Toward a Prosecutor for the European Union, Volume 1: A Comparative Analysis* (Oxford: Hart, 2012); M. Kusak, 'Mutual Admissibility of Evidence and the European Investigation Order: Aspirations Lost in Reality' (2019) 19(1) *ERA Forum: Journal of the Academy of European Law* 391; in this sense, globalisation and digitalisation seem to have outpaced even the caution expressed by authoritative scholars in the aftermath of the Green Paper adoption (see, e.g., reactions to the Green Paper by Professor John Spencer as reported in S. Allegrezza, 'Critical

It is true that harmonisation may still be indirectly achieved thanks to the application of mutual recognition tools. In other words, in order to facilitate the execution of measures issued within the area of security, freedom and justice, member states may be informally incentivised to agree upon minimum common procedural standards. The underlying idea is that compliance with the latter should in principle reduce the risk of an executing member state invoking grounds for refusal to oppose an order issued by another state. This way of proceeding towards harmonisation, however, is neither structural nor truly foreseeable in its development. At the very least, it requires a certain amount of time (and of judicial decision making) before producing consolidated results. For these reasons, the creation of common procedural standards through this process remains rather occasional, and only seldomly able to produce rules that concern admissibility.⁷⁴

As will be argued further, some examples in this sense have recently emerged in the case-law of the CJEU. Nonetheless, much more could be achieved within the EU, especially given the fact that lack of legislation in this field relies heavily upon political rather than legal reasoning.

Indeed, Article 82(2) of the Treaty on the Functioning of the European Union (TFEU) already provides for the legal bases which would allow the EU to adopt ‘minimum rules’ on the ‘mutual admissibility of evidence’.⁷⁵ Thus, although only ‘to the extent necessary to facilitate mutual recognition’, harmonisation of admissibility rules for (digital) evidence is an objective that could already be met in the EU, without any need for further institutional amendments.⁷⁶

5.5 LOOKING FOR ADMISSIBILITY CRITERIA IN THE EUROPEAN CASE-LAW

Against the political obstacles to a common harmonising legislation on the admissibility of evidence in the EU, and a persistent need for common rules on the matter, especially concerning digital data, jurisprudence has acquired a great role. This is the case for domestic courts, but even more so for the ECtHR and the CJEU.

Keeping the focus on the supranational level, analysis of the relevant decisions reveals the seemingly different attitudes of the two European courts. On one side, the ECtHR, which has long since touched upon the matter, shows a rather restrictive approach that affects only to a very limited extent the discretion of member states in establishing admissibility rules. On the other side, the CJEU, which has started to address the issue only more recently, and yet never with the

Remarks on the Green Paper on Obtaining Evidence in Criminal Matters from One Member State to Another and Securing Its Admissibility’ (2010) 9 *Zeitschrift für Internationale Strafrechtsdogmatik* 578 n. 577).

The phenomenon has recently started to be measured by Eurojust, again with regard to the EIO Directive, see Eurojust, *Report on Eurojust’s Casework in the Field of the European Investigation Order*, 24 November 2020, 28, www.eurojust.europa.eu/sites/default/files/2020-11/2020-11_EIO-Casework-Report_CORR_.pdf.

⁷⁴ As shown, for instance, by the more consolidated practice of the European arrest warrant with regard to certain procedural profiles, such as trial *in absentia*, on which see H. Brodersen, V. Glerum and A. Klip, *Improving Mutual Recognition of European Arrest Warrants for the Purpose of Executing Judgments Rendered Following a Trial at which the Person Concerned Did Not Appear in Person* (InAbsentieAW, 2020), www.inabsentieaw.eu/wp-content/uploads/2020/02/InAbsentieAW-Research-Report-1.pdf; and G. Giudicelli-Delage and S. Manacorda (eds.), *L’intégration pénale indirecte: Interactions entre droit pénal et coopération judiciaire au sein de l’Union Européenne* (Paris: Société de Législation comparée, 2005). With regard to the EIO, for instance, see the case of real-time monitoring of banking records, M. Caianiello, ‘L’attuazione della direttiva sull’ordine europeo di indagine penale e le sue ricadute nel campo del diritto probatorio’ (2018) 6 *Cassazione penale* 2197.

⁷⁵ Highlighting the crucial role played against this initiative by member states, see Bachmaier Winter, ‘European Investigation Order’, 580, 581; more recently, Vervaele, ‘Lawful and Fair Use of Evidence’, 91 ff.; and Ligeti et al., ‘Admissibility of Evidence’, 205.

⁷⁶ ‘The EU legislator should accept its responsibility and submit a proposal for a directive under Article 82(2)(b–c) TFEU, with the aim of harmonising the standards for the admissibility of evidence and unlawful evidence’, Vervaele, ‘Lawful and Fair Use of Evidence’, 93.

explicit intent of establishing harmonised rules, displays a relatively proactive attitude in this regard. Both courts, in any case, took their lead from a common ground, developing their case-law on admissibility mostly from a privacy-oriented perspective, rather than a criminal procedure one, focused on defence and fair trial rights.

The ECtHR mostly addresses the matter of digital evidence on the basis of Article 8 of the ECHR, which protects the right to private life. For many years now, the Court has expanded the scope of this provision to include also challenges deriving from technological development; thus, the Article represents an easy reference when addressing in general the legitimacy of investigative measures carried out also in the digital dimension.⁷⁷

Many of the ECtHR decisions grounded in Article 8 and referring to digital evidence, however, show a rather self-restrictive approach and refer to a rather limited subject matter: that of search and seizure of digital data belonging to a defence counsel.⁷⁸ In *Sallinen and o. v. Finland* (2005), for instance, the Court affirmed that it is firstly national courts that should rule over the compliance of domestic legislation with fundamental rights.⁷⁹ This perspective, rather unusual in light of other Article 8 jurisprudence, offered a very narrow interpretation of the level of protection to the individuals affected by digital investigations. For one thing, although the existence of a proper legal basis for the search and seizure of digital data was among the issues raised by the applicant, the Court limited itself to uncritically supporting the claim made by national courts that such legal basis did exist. No further autonomous examination was carried out about the adequacy of the legal basis in qualitative terms.⁸⁰ Similar considerations apply also to the following case-law. In *Wieser and Bicos Beteiligungen GmbH* (2007), for example, search and seizure of all business documents was ordered in the applicant company.⁸¹ Although domestic law did not contain specific provisions for the search and seizure of electronic data, national case-law supported the use of these measures based on an analogic application of the regulation referring to physical objects. Such a position was again uncritically accepted by the ECtHR, which considered it a sufficient legal basis to limit the right to privacy.⁸²

This narrow interpretation seems, however, rather problematic. Firstly, the acritical acceptance of the carrying out of digital investigations without a proper legal basis

⁷⁷ See, e.g., *Tapia Gasca and o. v. Spain*, Appl. no. 20272/06, 22 December 2009, § 111; *Diamante and Pelliccioni v. San Marino*, Appl. no. 32250/08, 27 September 2011, § 151; *Anghel v. Italy*, Appl. no. 5968/09, 25 June 2013, § 69.

⁷⁸ D. J. Harris, M. O'Boyle, E. P. Beates and M. Buckley, *Law of the European Convention on human Rights*, 4th ed. (Oxford: Oxford University Press, 2018), 536 ff.

⁷⁹ See *Sallinen and o. v. Finland*, Appl. no. 50882/99, 27 September 2005, §§ 77–79, concerning the situation in which the accused, a lawyer, had the computers of his law firm searched and seized in a criminal investigation on aggravated debtor's fraud. Despite the presence of general critical issues related to the actual relevance of the seized data, the Court focused much of its judgment on the level of protection recognised in Finnish law of the attorney-client privilege, sparing only a few considerations for the legitimacy of the digital investigation technique itself.

⁸⁰ *Sallinen and o. v. Finland*, § 77.

⁸¹ *Wieser and Bicos Beteiligungen GmbH v. Austria*, Appl. no. 74336/01, 16 October 2007, where a company filed an appeal before national authorities, complaining, among other things, that the search report did not mention which electronic data had been copied and seized, and that it had not been signed by all the officers who had been present at the search. Infringement of the rights of professional secrecy was also raised by Wieser, a lawyer who held the position of general manager of that company.

⁸² *Wieser and Bicos Beteiligungen GmbH v. Austria*, § 53. The occurrence of potential procedural breaches was examined by the Court exclusively in light of the proportionality principle. In this sense, a violation of the Convention was found because of a 'striking' asymmetry between the treatment granted to physical and digital evidence: as claimed by the defendants, procedural rules for the search and seizure of 'physical objects' had indeed not been fully complied with in the specific case with regard to digital evidence (§ 63). A similar approach was followed in, e.g., *Robathin v. Austria*, Appl. no. 30457/06, 3 July 2012, §§ 47 and 52, where a violation of Article 8 was grounded in the disproportionate vagueness of the search warrant. The latter allowed the police to search and examine all documents of the defendants, and not just those strictly connected to the offence at stake. Considering, however, that in *Wieser and Bicos Beteiligungen GmbH v. Austria* (§ 59) the Court had upheld as 'reasonable'

might raise some resistance in light of civil law traditions (common to most EU member states), according to which compliance with the rule of law necessarily requires the legal basis to be grounded in statutory law. Secondly, the interpretation of the ECtHR in this matter, apparently clashing with the prescriptions of the Budapest Convention,⁸³ seems also rather unsatisfactory against the same Strasbourg jurisprudence. The Court has indeed clarified that, even in systems which do not recognise the *stare decisis*, case-law may represent a legitimate legal basis in criminal proceedings, but only as long as its content is foreseeable by the defendant, and that occurs only where the latter is sufficiently consolidated.⁸⁴ The check, however, was not performed in any of the examined cases, where the Court limited itself to registering the existence of case-law, without any assessment of the ‘quality’ of the latter. The fact that, when it comes to digital evidence, the Court does not seem to consider it necessary to verify whether the relevant legal basis really possesses the quality required to ensure an effective protection of the rights at stake appears quite worrisome. Such a minimalistic approach is indeed far from satisfactory, especially in light of the numerous and particular vulnerabilities of digital evidence illustrated already.

Looking for hints on admissibility criteria for digital evidence, the examined case-law cannot but produce a sense of disappointment. This conclusion is not refuted also by trying to relate the interpretation of Article 8 to the jurisprudence concerning evidence in criminal proceedings. Indeed, the impact of the ECtHR case-law on admissibility rules appears even lower when it comes to Article 6 of the ECHR.

Under this profile, the Court has dealt with the matter of digital investigations only indirectly, and mostly with respect to potential violations of the adversarial principle in the form of limited access to the evidence. In such jurisprudence, though, the ECtHR did not really seek to establish admissibility criteria and instead reiterated the prominence of an ‘overall approach’ in assessing potential violations to the defence rights.⁸⁵

Actually, the Court has repeatedly stated how Article 6 ‘does not lay down any rules on the admissibility of evidence or the way it should be assessed’.⁸⁶ Thus, besides cases where the cause of inadmissibility falls under the absolute prohibition of torture or inhuman and degrading treatment (Article 3 of ECHR), judges in Strasbourg tend to leave the matter within the margin

a search warrant issued against ‘any business documents revealing contacts with the suspects’, the burden on the investigators set by the ECtHR in this regard does not seem particularly demanding.

⁸³ See Section 5.4.

⁸⁴ See *Contrada v. Italy* (No. 3), Appl. no. 66655/13, 14 April 2015, §§ 70–76.

⁸⁵ *Van Wesenbeeck v. Belgium*, Appl. nos. 67496/10 and 52936/12, 23 May 2017, §§ 67–68; *Natunen v. Finland*, Appl. no. 21022/04, 31 March 2009, §§ 42–43; *Sigurður Einarsson and others v. Iceland*, Appl. no. 39757/15, 4 June 2019, § 85 ff., on which see L. Bartoli, ‘Parità delle armi e e-discovery nel processo penale’, in R. Brighi (ed.), *Nuove questioni di informatica forense* (Rome: Aracne, 2022), 89 ff.

⁸⁶ *Garcia Ruiz v. Spain*, Appl. no. 30544/96, 21 January 1999, § 28. See also *Schenk v. Switzerland*, Appl. no. 10862/84, 12 July 1988, §§ 45–46; *Miailhe v. France* (No. 2), Appl. no. 18978/91, 26 September 1996, § 43; *Heglas v. the Czech Republic*, Appl. no. 5935/02, 1 March 2007, § 84; *Moreira Ferreira v. Portugal* (No. 2), Appl. no. 19867/12, 11 July 2017, § 83, on which see S. Gless, ‘Mutual Recognition, Judicial Inquiries, Due Process and Fundamental Rights’, in J. A. E. Vervaele (ed.), *European Evidence Warrant – Transnational Judicial Inquiries in the EU* (Antwerp: Intersentia, 2005), 124; Z. Durdevic, ‘Admissibility of Evidence, Judicial Review of the Actions of the European Public Prosecutor’s Office and the Protection of Fundamental Rights’, in V. Bazzocchi (ed.), *Protecting Fundamental and Procedural Rights: From the Investigation of OLAF to the Future EPPO*, 2nd ed. (Rome: Fondazione L. Basso, 2014), 126; J. McBride, *The Case Law of the European Court of Human Rights on Evidentiary Standards in Criminal Proceedings*, on the European Union–Council of Europe Joint Project, ‘Application of the European Convention on Human Rights and Harmonisation of National Legislation and Judicial Practice in Line with European Standards in Georgia’, 24, <https://rm.coe.int/council-of-europe-georgia-european-court-of-human-rights-case-study-ev/16807823c3>.

of discretion of the states.⁸⁷ Legal scholars have thus rightly highlighted how, in this field, ‘solutions offered by the ECtHR [do] not always offer the best protection to human rights’.⁸⁸

On the contrary, the approach of the Court of Justice to the matter appears relatively more promising. To start with, in a series of landmark decisions about data retention, the CJEU showed an interesting standing on this very delicate subject.⁸⁹ In *La Quadrature du Net* (2020), the Court stated that, in principle, it is up to national judges to determine the adequacy of domestic rules on the admissibility and use of evidence.⁹⁰ Regardless of such a formal recognition, national legislators are, however, limited in their assessment by the principle of effectiveness. Interestingly, the CJEU explicitly linked such a principle with that of fairness, and in particular with the ‘adversarial principle and, therefore, the right to a fair trial entailed by the admissibility of such information and evidence’.⁹¹ In light of the above, should evidence be obtained in violation of said safeguards (for instance, because of the violation of the right to be heard, i.e. if a party is not in a position to comment effectively on it), the piece of information shall be ‘excluded’ and ‘disregarded’.⁹² Starting from parameters similar to those identified in the ECtHR jurisprudence, therefore, the CJEU seems to draw clearer and more foreseeable conclusions from the potential violation of said principles. The position was reiterated in the subsequent case-law, such as in *Prokuratuur* (2021)⁹³ and *G.D. v. Commissioner of An Garda Síochána* (2022).⁹⁴

Furthermore, here the CJEU undertook a safeguarding approach concerning admissibility of evidence not only with respect to data retention but also with a closer reference to criminal proceedings as well.⁹⁵ In *WebMindLicence* (2015), dealing with the problems raised by information sharing between criminal and administrative proceedings, the Court established a double-proportionality test in order to assess the admissibility of evidence. According to it, the judge had

⁸⁷ Besides, even in cases of a breach of Article 3 ECHR, the Court limited the scope of the inadmissibility and did not embrace the theory of the fruits of the poisonous tree (on which see S. C. Thaman, ‘Fruits of the Poisonous Tree in Comparative Law’ (2010) 16 *Southwestern Journal of International Law* 333); see famously *Gäfgen v. Germany*, Appl. no. 22078/05, 1 June 2010, §§ 98–99. For a recollection of the case-law in this regard, see, e.g., McBride, *The Case Law of the European Court of Human Rights*, 25.

⁸⁸ Allegrezza, ‘Critical Remarks on the Green Paper’, 575.

⁸⁹ For a reconstruction of the jurisprudence of the Court in the field, see recently, M. Catanzariti, ‘Procedural Rights through the Lenses of Data Protection’, in G. Contissa, G. Lasagni, M. Caianiello and G. Sartor (eds.), *Effective Protection of the Rights of the Accused in the EU Directives: A Computable Approach to Criminal Procedure Law* (Leiden: Brill, 2022), 259 ff.

⁹⁰ Indeed,

the objective of national rules on the admissibility and use of information and evidence is ... to prevent information and evidence obtained unlawfully from unduly prejudicing a person who is suspected of having committed criminal offences. That objective may be achieved under national law not only by prohibiting the use of such information and evidence, but also by means of national rules and practices governing the assessment and weighting of such material, or by factoring in whether that material is unlawful when determining the sentence. (Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net* and Others v. Premier ministre and Others [2020] ECLI:EU:C:2020:791, § 225)

⁹¹ *La Quadrature du Net*, § 226.

⁹² *Ibid.*, § 226–227: ‘where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact’.

⁹³ Case C-746/18, *H.K. v. Prokuratuur* [2021] ECLI:EU:C:2021:152, § 44.

⁹⁴ Case C-140/20, *G.D. v. Commissioner of An Garda Síochána* [2022] ECLI:EU:C:2022:258, § 115 ss.

⁹⁵ Naturally, the topic is also relevant in other fields of law under the competence of the CJEU: competition law, above all. In that domain, however, explicit legal bases can be found (see Art. 12 of Council Regulation (EC) No. 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, [2003] OJ L 1, 4 January 2003); Case T-54/14, *Goldfish BV v. European Commission* [2016] ECLI:EU:T:2016:455 and Case C-469/15 P, *FSL Holdings and Others v. European Commission* [2017] ECLI:EU:C:2017:308, on which see Vervaele, ‘Lawful and Fair Use of Evidence’, 73 ff.; M. Simonato, ‘Illicit but Admissible Evidence’, *EU Law Enforcement*, 31 October 2016, <https://eulawenforcement.com/?p=98>.

to verify whether ‘the use [of the exchanged information] is proportionate to the aim pursued, examining whether all the necessary information could not have been obtained by means of investigation that interfere less’ with the rights at stake (Art. 7 of the Charter of Fundamental Rights of the European Union (CFREU)). If that requirement is not satisfied, ‘the evidence obtained in the context of the criminal procedure and used in the administrative tax procedure must be disregarded and the contested decision which is founded on that evidence must be annulled if, as a result, the decision has no basis’.⁹⁶

More recently, several preliminary questions in the famous Encrochat investigation were referred to the Court of Justice. In this case encrypted data was collected through the hacking of a server, also thanks to the use of AI technology.⁹⁷ In her opinion, Advocate General Capeta proposed a restrictive approach, along the lines set out by the ECtHR. In her view, ‘EU law does not govern the admissibility of evidence in criminal procedures’.⁹⁸ Therefore, it is impossible to induct any principles from the Charter as far as the admissibility of evidence in criminal proceedings is concerned.⁹⁹ While this approach presents the problems already highlighted with regard to the ECtHR case-law, alternative options available to the Court may also raise some critical concern. For instance, should the CJEU follow the jurisprudence already developed in the ‘data retention saga’, as it is likely to do, criticisms could be made about the relevance given to the right to be heard, that is, the possibility for the parties to comment upon the use of a certain piece of evidence. It is not clear, in particular, what information should be made available to the parties to make the possibility to comment an effective safeguard (an aspect that is especially tricky in the Encrochat case, where national defence interests were also at stake). Merely referring to this right, therefore, may end up resembling another very controversial approach of the ECtHR, which considers the right to be heard among the range of potential ‘counterbalancing measures’ capable of reducing the finding of violations of Article 6 ECHR.¹⁰⁰ Legal scholars have already pointed out the problematic aspects of this position: from the debasement of the individual aspects composing the right to a fair trial, violations of which could now be mutually compensated, to the loss of legal foreseeability about the minimum level of procedural rights protection, which could result in a violation of these rights.¹⁰¹

⁹⁶ Case C-419/14, *WebMindLicenses Kft. v. Nemzeti Adó- és Vámhivatal Kiemelt Adó- és Vám Főigazgatóság* [2015] ECLI:EU:C:2015:832, §§ 82–89, according to which a first proportionality assessment shall be carried out by the criminal court where the evidence was collected, and then by the administrative court receiving that evidentiary material. On the possibility of applying this double test also in the opposite case (where a piece of evidence is transferred from an administrative to a criminal proceeding), see S. Tesoriero, ‘Processo penale e prova multidisciplinare europea in materia di illeciti finanziari’ (2016) 6 *Rivista di diritto processuale* 1526 ff.

⁹⁷ For a reconstruction of this complex and multi-level investigation, see, *ex multis*, Jan-Jaap Oerlemans, ‘The Future of Data-Driven Investigations in Light of the Sky ECC Operation’ (2023) 14(4) *New Journal of European Criminal Law* 434–458; Georgios Sagittae, ‘On the Lawfulness of the EncroChat and Sky ECC-Operations’ (2023) 14(3) *New Journal of European Criminal Law* 273–293.

⁹⁸ Opinion of AG Tamara Capeta, of 26 October 2023, Case C-670/22, *Staatsanwaltschaft Berlin v. M.N.*, para. 117.

⁹⁹ *Ibid.*, para. 116 ff.

¹⁰⁰ See ECtHR, *Schatschaschwili v. Germany* App No. 9154/10, 15 December 2015, paras. 107, 114–116, 125–131; ECtHR, *Ibrahim and others v. The United Kingdom* App Nos. 50541/08, 50571/08, 50573/08 and 40351/09, 13 September 2016, para. 274; ECtHR, *Murtazaliyeva v. Russia* App No 36658/05, 18 December 2018, paras. 167–168. On the overall approach applied to surveillance matters, see ECtHR, *Big Brother Watch and others v. The United Kingdom* App Nos. 58170/13, 62322/14 and 24960/15 (GC), 25 May 2021, paras. 360 and 370; ECtHR, *Case of Centrum för Rättvisa v. Sweden* App No. 35252/08, 25 May 2021, para. 274. See further L. Bachmaier Winter, ‘Proportionality, Surveillance and Criminal Investigation: Strasbourg Court Facing Big Brother’, in E. Billis, N. Knust and A. Rui (eds.), *The Principle of Proportionality in Crime Control and Criminal Justice* (Oxford: Hart, 2021), 317.

¹⁰¹ See, e.g., T. Mariniello, ‘Too Much Unfairness in the “Overall Fairness” Test (Murtazaliyeva v Russia)’, in T. Mariniello (ed.), *Judge Pinto de Albuquerque and the Progressive Development of International Human Rights Law* (Leiden: Brill-Nijhoff, 2021), 231; M. Caianiello, ‘You Can’t Always Counterbalance What You Want’ (2017) 25(4) *European Journal of Crime, Criminal Law and Criminal Justice* 283.

The idea that the CJEU could also start sharing a similar ‘overall approach’, considering the right to be heard as a sort of ‘admissibility trigger’, might thus shed, from a different angle, another problematic light on the protection of fair trial rights throughout the Union.

Still, from a broader perspective, at least the *Encrochat* case is likely to officially recognise the urgency of common rules on mutual admission of evidence, also in the (purely) criminal domain.

In the gap left by the European legislator, the Court in Luxembourg finally seems to have, perhaps reluctantly but steadily, taken up the task of introducing some basic but transnational and common criteria concerning the admissibility of evidence. In most of the relevant cases the chance to do so emerged precisely because of the need to deal with digital information, and this brings us back to one of the initial queries: should digital evidence be the subject of specific admissibility rules?

5.6 WHICH WAY FORWARD?

This chapter took its lead from three main questions: are there legal bases which support the establishment of transnational admissibility rules in the EU? Should such rules be specific for digital evidence? And, in any case, what should they look like?

While the answer to the first question is, at least in principle, rather straightforward in light of Article 82(2) TFEU, the approach to the latter two is more speculative against the current legal framework. Indeed, not only European legislation on the matter is *de facto* inexistent; the national level is definitely divergent too when it comes to law of evidence in general, and admissibility criteria in particular.¹⁰² Domestic systems tend not to provide for specific regimes on the admissibility of e-evidence, and rather to rely on general rules applied by analogy. Besides this very general consideration, however, national legal frameworks appear too scattered to clearly extrapolate a shared regulatory approach.¹⁰³

¹⁰² Indeed, though,

looking back at the rationale of the concept of the admissibility of evidence, we can state that the ECtHR and the EU Courts mostly use a systemic integrity model with a balancing approach (the judicial integrity approach). This means that they only resort to the exclusion of evidence for serious violations of important rights and only in cases where the dismissal of the charges will not significantly undermine the justice interest in convicting those who have committed serious crimes. (Vervaele, ‘Lawful and Fair Use of Evidence’, 79)

Several exceptions find application in the model, and both the latter and the exceptions are differently implemented at the national level: see, *ex multis*, M. Delmas-Marty and J. R. Spencer (eds.), *European Criminal Procedures* (Cambridge: Cambridge University Press, 2002), 594 ff.; M. Delmas-Marty and J. A. E. Vervaele (eds.), *The Implementation of the Corpus Juris in the Member States* (Utrecht: Intersentia, 2000); British Law Society, *Study of the Laws of Evidence in Criminal Proceedings throughout the European Union*, Study for the European Commission’s Directorate General for Justice and Home Affairs, 2004; European Parliament, *Criminal Procedural Laws Across the European Union – A Comparative Analysis of Selected Main Differences and the Impact They Have Over the Development of EU legislation*, August 2018, 48 ff; Vervaele, ‘Lawful and Fair Use of Evidence’, 56 ff.; S. Gless and T. Richter (eds.), *Do Exclusionary Rules Ensure a Fair Trial? A Comparative Perspective on Evidentiary Rules* (Cham: Springer Open, 2019); Durdevic, ‘Admissibility of Evidence’, 126; S. C. Thaman (ed.), *Exclusionary Rules in Comparative Law* (Dordrecht: Springer, 2013); C. Slobogin, ‘A Comparative Perspective on the Exclusionary Rule in Search and Seizure Cases’ (9 April 2013) Vanderbilt Public Law Research Paper No. 13-21, <https://ssrn.com/abstract=2247746>.

¹⁰³ Bartoli and Lasagni, ‘Antifraud Investigation and Digital Forensics’, 201 ff. Nonetheless, attempts are currently underway to ease the context, see, e.g., European Law Institute (ELI), Admissibility of E-Evidence in Criminal Proceedings in the EU, www.europeanlawinstitute.eu/projects-publications/current-projects/current-projects/admissibility-of-e-evidence/.

This does not mean, however, that finding common ground for the admissibility of evidence is an unrealistic goal: to this end, the broad awareness of the need for a common response when it comes to digital evidence, to ensure a consistent application of fundamental rights throughout the Union, could provide a formidable impulse. It is perhaps not a coincidence that the jurisprudence of the CJEU mostly refers to digital data that calls for member states to exclude evidence collected in violation of the principle of proportionality or of fair trial rights.

The Court, however, did not provide for a list of specific procedural requirements that should be complied with in order to ensure the use at trial of (digital) evidence. In this gap, a potential role in shaping admissibility rules could be found in the methodology used to collect the information that, as previously illustrated, plays a crucial role in determining the reliability of the information collected in the digital dimension.

This is not to suggest that technical standards should be incorporated by statutory law: for one, no regulatory provision could ever evolve fast enough to keep pace with the technological evolution of the specific devices and tools which are to be applied and examined in digital forensics. However, there are reasons to make more explicit the link between compliance with technical standards and admissibility rules.

Given the expert features of digital evidence, the idea that judicial discretion alone could be enough to remedy potential inadmissibility issues is not without limits. The activity of the judiciary needs indeed to be put into context. As is often the case in the EU member states, legal operators, and especially judges, may not systematically receive adequate training in digital forensic expertise; or technical standards may not be accessible (or accessible enough) to the parties of the proceedings.¹⁰⁴ Against this state of play, legal scholars have highlighted the risk for judicial discretion to simply act as a way to replace ‘junk science’ with ‘junk rulings’.¹⁰⁵ Such a consideration, furthermore, does not touch only upon the domain of digital data but could be extended to the whole domain of forensic evidence.

Should this argument be brought to the point of creating in the EU an admissibility rule, according to which digital evidence shall not be used at trial if it has been collected in violation of best technical practices? And should such a rule be limited to digital evidence or extended to all forensics contributions to criminal proceedings?

In Europe, this approach has not yet found an equivalent in statutory law, neither at the supranational nor at the domestic level. Namely, although all systems consistently state that digital evidence ought to be reliable and authentic, these requirements rarely have straightforward repercussions for the admissibility at trial.¹⁰⁶

¹⁰⁴ Bartoli and Lasagni, ‘Antifraud Investigation and Digital Forensics’, 217 ff. Also supporting the need to structurally integrate such knowledge and scientific methodology in a proper epistemological framework and in the training of legal operators, G. Ubertis, *Profili di epistemologia giudiziaria* (Milan: Giuffrè, 2015), 30 ff.; R. Bhaskar, ‘State and Local Law Enforcement Is Not Ready for a Cyber Katrina’ (2006) 49(2) *Communications of the ACM* 81–83.

¹⁰⁵ See P. J. Neufeld, ‘The (Near) Irrelevance of Daubert to Criminal Justice: And Some Suggestion for Reform’ (2005) 95(Supp. 1) *American Journal of Public Health* 107 ff.; K. R. Berman, ‘Daubert Turning 20: Junk Science Replaced by Junk Rulings?’, ABA Section of Litigation Annual Conference, 18–20 April 2012; P. Huber, *Galileo’s Revenge: Junk Science in the Courtroom* (New York: Basic Books, 1991); S. Jasanoff, ‘Law’s Knowledge: Science for Justice in Legal Settings’ (2005) 95 *American Journal of Public Health* 66.

¹⁰⁶ For the European level, see Section 5.4. For the national level, even where specific standards are in place, their breach does not necessarily have an impact on the admissibility of the collected data: Illustrative, in this sense, is the Spanish system (on which see Bachmaier Winter, ‘The Handling of Digital Evidence in Spain’, 201 ff.), where in 2003 the Constitutional Court concluded that violations of the chain of custody (in the specific case, digital data seized from a computer during a home search that was not correctly identified and sealed) could amount to a breach of fair trial rights because potential data manipulations or alterations in this way can no longer be excluded. To achieve that, however, the defendant cannot simply rely on the onus for the prosecutor to prove the soundness of the

In particular, while the possibility for national judges to exclude a piece of (digital) evidence is generally recognised in the member states, its exercise often largely depends on the discretion of the judicial authority.¹⁰⁷ A declaration of inadmissibility, thus, is not a clearly foreseeable outcome for the defendant.¹⁰⁸ This is even more so in transnational proceedings, where access to the relevant case-law may be further impaired by a different legal culture or a different language.¹⁰⁹

Some elements in favour of a more explicit approach to the matter, however, emerge from some of the sources analysed so far. For instance, the mentioned EU standards (ENISA *Basic Guide* and OLAF *Guidelines*) seem to implicitly suggest a reading that subjects the fairness of digital investigations to compliance with a series of technical requirements (e.g. basic qualification for first responders; video recording of digital forensics operations; the need to produce a non-alterable chain of custody; the information rights of the party whose device is at stake; the maximum duration of retention of the collected data).¹¹⁰ The suggestion is implicit, true, but this is hardly surprising, considering that neither ENISA nor OLAF has the power to interfere with national criminal procedure law.

The link between compliance with technical standards and admissibility is then even more explicit in the Council of Europe's *Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges*. According to it, a connection is recognised between adoption of proper technical procedures and use of the evidence in court, with allocation of the burden of proof to the prosecutor. Putting this perspective into practice within digital investigations could directly affect the admissibility of evidence. For instance, where the prosecutor is not able to prove the adherence of some digital forensic operations to the relevant best practices, the defence could claim the inadmissibility of the information collected.

A similar approach towards admissibility rules is, moreover, reflected in the way other judicial systems tend to deal with forensic evidence. In several Latin American countries, for instance, provisions can be found in the criminal procedure codes, according to which special admissibility conditions are established, including the need to assess the 'reliability of expert knowledge'.¹¹¹ The reference is even clearer in the USA, where such an approach finds direct legal bases both in statutory law and in the jurisprudence. For instance, according to the US Federal Rules of Evidence, 'to satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is'. The onus is especially relevant with regard to forensic evidence,

adopted technical procedure and shall propose an alternative expert evidence and challenge the opinion prepared by the investigators (STS 170/2003 of 29 September, see also STS 491/2016 of 8 June). In subsequent case-law of 2012, the same Court further clarified that, although the regularity of the chain of custody is essential to assess the authenticity of digital evidence, the latter may be excluded subject to an assessment of the gravity of the infringement (STS 1072/2012 of 11 December).

¹⁰⁷ See, e.g., Vervaele, 'Lawful and Fair Use of Evidence', 79.

¹⁰⁸ Ibid., 60, recalling how '[a]lready from the terminology we see that the rationale behind the assessment of unlawful evidence and related consequences might differ from country to country'.

¹⁰⁹ Although, also in this regard, applicative research is currently being carried out to fill such gaps; see, e.g., the platform for legal support and advice built within the CrossJustice project (847346 – JUST-JACC-AG-2018), www.crossjustice.eu. The results of the research are published in G. Contissa, G. Lasagni, M. Caianiello and G. Sartor (eds.), *Effective Protection of the Rights of the Accused in the EU Directives: A Computable Approach to Criminal Procedure Law* (Leiden: Brill, 2022).

¹¹⁰ See Section 5.3.2.

¹¹¹ See the cases of Chile (Arts. 314 and 316), Argentina (Arts. 263 No. 3 of CCP de la Nación, 250 No. 3 of CCP de Provincia de Buenos Aires and 134 of CCP de ciudad de Buenos Aires), Colombia (Art. 422) and, in a more nuanced way, Peru (Art. 174.1) and Guatemala (Art. 227), on which see M. Duce, *La prueba pericial* (Buenos Aires: Ediciones Didot 2013), 79–80.

as in this case the same Rules require the latter to be the ‘product of reliable principles and methods’.¹¹² This approach was further strengthened by the US Supreme Court (USSC). In the landmark decision *Daubert v. Merrell Dow Pharmaceuticals Inc* (1993), the Court had to assess the admissibility of the testimony given by an expert witness (in the specific case: on whether a certain prescription drug could cause birth defects in children). Taking a stand on the matter, the USSC affirmed that expert evidence is admissible only upon showing that the scientific methods it is based on are proven to be ‘valid’. To prove this, the Court established a set of factors to be considered, namely: (1) whether the theory or technique in question can be and has been tested; (2) whether it has been subjected to peer review and publication; (3) its known or potential error rate; (4) the existence and maintenance of standards controlling its operation; and (5) whether it has attracted widespread acceptance within a relevant scientific community.¹¹³ These so-called *Daubert* criteria thus represent an interesting elaboration of admissibility rules, tailored to the exigencies emerging from the use of forensic evidence.¹¹⁴

Against the legal framework reconstructed in the previous paragraphs, the EU could also be ready to adopt a common and clearer rule on the matter. In this sense, digital evidence, with its specificity, could represent the best chance to create a first common, minimum rule of admissibility for forensics evidence. According to it, a piece of information shall be admissible only if the methodology used to collect it can be considered scientifically valid.

Of course, such a rule does not abruptly solve all potential problems related to expert evidence, including those involving digital data. In fact, it might even aggravate the situation further (for

¹¹² See, respectively, US Federal Rules of Evidence (2019), Rules 901 and 702.

¹¹³ *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 US 579 (1993). In 1999, this case-law was extended also to expert ‘non-scientific’ technical testimony, see *Kumho Tire Co. v. Carmichael*, 526 US 137 (1999). Although *Daubert v. Merrell Dow Pharmaceuticals* is by far the most renowned on the matter, this decision represents only the last part of a rather long series of criteria, historically developed by the US Courts, starting from *Frye v. United States*, 293 F. 1013 (D.C. Circ. 1923); *Coppolino v. State*, 223 So 2d 68, 75 (Fla. Dist. Ct. App. 1969); *People v. Kelly*, 549 P 2d 1240 (S. Ct Cal. 1976). Among the extensive literature on *Daubert v. Merrell Dow Pharmaceuticals*, see M. J. Saks, ‘The Aftermath of Daubert: An Evolving Jurisprudence of Expert Evidence’ (2000) 40(2) *Jurimetrics* 229; E. K. Cheng and A. H. Yoon, ‘Does Frye or Daubert Matter? A Study of Scientific Evidence Admissibility Standards’ (2005) 91 *Virginia Law Review*, 471; L. A. Vickers, ‘Daubert, Critique and Interpretation: What Empirical Studies Tell Us About the Application of Daubert’ (2005) 40 *University of San Francisco Law Review* 137; Neufeld, ‘The (Near) Irrelevance of Daubert’, 107 ff.; S. Walker, ‘Drawing on Daubert: Bringing Reliability to the Forefront in the Admissibility of Eyewitness Identification Testimony’ (2013) 62(4) *Emory Law Journal* 82, 1205, 1207.

¹¹⁴ Though focusing only on the reliability and usefulness of the evidence does not necessarily addresses all problematic issues on its admissibility. See, e.g., R. J. Allen and C. K. Smiciklas, ‘The Law’s Aversion to Naked Statistics and Other Mistakes’ (2022) 28(3) *Legal Theory* 18, noting how ‘the modern treatment of statistics in American litigation involves overwhelming acceptance of the evidence so long as it reliable and helpful — even when the evidence is as close to being “naked” as possible. Rather than applying some special rule to statistical evidence, courts across the country treat it like any other evidence.’ Moreover, the application of the *Daubert* criteria has lately been disregarded with regard to some kind of forensic evidence, namely automated generated ones. See, e.g., the famous decision *State of Wisconsin v. Loomis*, 881 N.W. 2d 749 (Wis. 2016), which rejected the doctrine in case of automated risk-assessment tools measuring recidivism risk. The decision has been widely commented on and criticised in US and European literature: see, *ex multis*, ‘State v. Loomis. Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing. Recent Case: 881 N.W.2d 749 (Wis. 2016)’ (2017) 130(5) *Harvard Law Review* 1350, <https://harvardlawreview.org/2017/03/state-v-loomis/>; J. B. Wall, K. A. Blanco, M. R. Dreeben, M. L. Goodspeed and S. A. C. Meisler, ‘Brief for the United States as Amicus Curiae in the Supreme Court of the United States Eric L. Loomis, Petitioner v. State of Wisconsin (No. 16-6387 Washington, DC, May 2017)’, www.scotusblog.com/wp-content/uploads/2017/05/16-6387-CVSG-Loomis-AC-Pet.pdf; I. De Miguel Beriain, ‘Does the Use of Risk Assessments in Sentences Respect the Right to Due Process? A Critical Analysis of the Wisconsin v. Loomis Ruling’ (2018) 17(1) *Law, Probability and Risk* 45–53; S. Quattrocchio, *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for a European Legal Discussion* (Cham: Springer, 2020), 166 ff.; Contissa and Lasagni, ‘When It Is (Also) Algorithms and AI’, 284 ff.

example, how can a non-expert judge assess the validity of a technical methodology?¹¹⁵). Legal systems, though, including those in the EU, are not new to such dilemmas,¹¹⁶ and anyway should be prepared to face them in light of the unavoidable integration between science and criminal justice.

It is hard to live up to such expectations. However, though slowly, a common understanding is finally emerging that recognises how, when it comes to digital, and in general to forensics evidence, the soundness of the methodology applied does matter. Leveraging Article 82(2) TFEU and the broad recognition given to the challenges posed by digital evidence, a minimum admissibility rule along this line could be created in the EU. It would be a first step towards building a minimum but harmonised evidence system that takes into account the increasing complexity of our modern, digital and globalised society.

¹¹⁵ F. Schauer, *The Proof: Uses of Evidence in Law, Politics, and Everything Else* (Cambridge, MA: Harvard University Press, 2022), 145 ff. The issue is emerging as especially critical with regard to AI technology, still largely unknown in its operation by legal practitioners, judges included, yet already used in several areas of investigation, as shown by the Encrochat/SKY ECC affair.

¹¹⁶ This is, for instance, the case in Italy, where in 2010 the Supreme Court adopted a test that includes *Daubert* (Cass. pen., sez. IV, 17 September 2010, No. 43786, *Cozzini*, on which see, e.g., C. Conti, 'Scienza controversa e processo penale: la Cassazione e il "discorso sul metodo"' (2019) 6 *Diritto penale e processo* 848 ff.; Gennari, 'I criteri di ammissione della prova scientifica', 186 ff.) or in Spain, see, e.g., J. Nieva-Fenoll, 'Repensando Daubert: La Paradoja de la Prueba Pericial' (2018) 9 *Civil Procedure Review* 11 ff. On the continuous challenges posed by science in judicial proceedings, see, *ex multis*, J. Hilbert, 'The Disappointing History of Science in the Courtroom: Frye, Daubert, and the Ongoing Crisis of "Junk Science" in Criminal Trials' (2019) *Faculty Scholarship* 460; J. J. Koehler, J. L. Mnookin, S. A. Cole, B. A. J. Fisher, I. E. Dror, M. Houck, K. Inman, D. H. Kaye, G. Langenburg, D. M. Risinger, N. Rudin and J. Siegel, 'The Need for a Research Culture in the Forensic Sciences' (2011) Faculty Working Papers 26, 26ff., <http://scholarlycommons.law.northwestern.edu/facultyworkingpapers/26>.

Exchange of Data between National Security Agencies and Law Enforcement

Challenges for Criminal Procedure

Tatiana Tropina

6.1 INTRODUCTION

The domains of national security and criminal law enforcement have fundamental differences in their scope and goals. Until relatively recently, in democratic societies, these regimes were strictly separated and governed by distinct frameworks. Yet, in the last two decades, the border between the two have blurred due to the transformation of complex crimes such as transnational organised crime and terrorism, which are increasingly being considered not only as a criminal justice issue but also as a national security threat.¹ These developments have been going hand-in-hand with the increasing reconsideration of the role of law enforcement in crime prevention and crime control. The primary focus in combating crime is gradually shifting from addressing offences that have already taken place to the idea of proactive and predictive ‘intelligence-driven’ policing.² These changes are facilitated by the increasing role of digital technology in transforming not only criminal behaviour but also ways to investigate and disrupt it. The availability of considerable volumes of digital data, which can help detect and investigate crimes, and the low cost associated with collecting, storing and analysing this data play a significant role in this transformation.³ Changing approaches to data gathering are driven by the belief that amassing as much information as possible can be an effective solution both in solving existing crime cases and in preventing future dangers in both national security and the criminal justice domain.⁴

The continuous drift of the previously separated regimes – national security agencies and law enforcement – closer to each other has led to the growing exchange of information between them. As one of the consequences, law enforcement agencies increasingly use data collected by national security services, including data gathered preventively, *ante delictum*⁵ and outside of

¹ Mar Jimeno-Bulnes, ‘The Use of Intelligence Information in Criminal Procedure: A Challenge to Defence Rights in the European and the Spanish Panorama’ (2017) 8 *New Journal of European Criminal Law* 171–191; Kent Roach, ‘The Eroding Distinction between Intelligence and Evidence in Terrorism Investigations’, in Nicola McGarrrity, Andrew Lynch and George Williams (eds.), *Counter-Terrorism and Beyond* (Abingdon: Routledge, 2010), 48–68; Angus Nurse, *The Citizen and the State: Criminal Justice and Civil Liberties in Conflict* (Bingley: Emerald, 2020), 6.

² Jacqueline Ross, ‘The Emergence of Foreign Intelligence Investigations as Alternatives to the Criminal Process: A View of American Counterterrorism Surveillance through German Lenses’, in Jacqueline Ross and Stephen Thaman (eds.), *Comparative Criminal Procedure* (Cheltenham: Edward Elgar, 2016), 475–476; Rosamunde van Brakel and Paul de Hert, ‘Policing, Surveillance and Law in a Pre-crime Society: Understanding the Consequences of Technology Based Strategies’ (2011) 20 *Cahiers Politistudies*, 166–167.

³ UN General Assembly, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/HRC/23/40, 17 April 2013, 10.

⁴ Van Brakel and de Hert, ‘Policing, Surveillance and Law’, 163–192.

⁵ Jimeno-Bulnes, ‘The Use of Intelligence Information’, 173.

criminal justice frameworks, in crime investigation and criminal proceedings.⁶ Despite this growing exchange of information between national security and law enforcement, the frameworks governing data collection in these two domains remain considerably different in terms of safeguards. These differences raise concerns about the potential violation of human rights in the criminal procedure by bypassing strict requirements for data collection established in criminal investigations.⁷

The national security architectures in various states can diverge significantly, with a multitude of frameworks and regulations governing distinctive structures involved in addressing threats to national security, crime prevention and crime control.⁸ While recognising the divergence, this chapter aims to provide a bigger picture of fundamental problems related to data exchange between intelligence agencies and law enforcement in criminal investigations. The chapter argues that the imbalance in scrutiny, accountability and oversight in two regimes of data collection – national security and criminal procedure – is inherent because they are fundamentally different in aim and function. When data collected by national security actors is shared with law enforcement agencies for the purpose of criminal investigation, the imbalance in scrutiny between the two regimes raises a fundamental question of circumventing safeguards established in the criminal procedure. There is an even more significant danger of using national security frameworks for data gathering as a substitute for collecting evidence in criminal investigations. While the flow of data between the two regimes is inevitable and constitutes a growing trend, the issue of proper safeguards should not be overlooked. On the contrary, due to disparities in the two regimes, robust measures for accountability and oversight must become an integral part of frameworks that enable or facilitate data flows from the national security domain to criminal investigations.

As the first step in building its argument, Section 6.2 of this chapter provides a broader context for discussion by highlighting the differences between the aims and the functions of the two traditionally separated national security and criminal justice regimes. Section 6.3 discusses how the changing threat landscape and the blurring borders between national security threats and crime are bringing these two separate regimes closer to each other. Section 6.4 focuses on the differences in safeguards between data collection for the purpose of national security and evidence gathering in criminal procedure and the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) concerning safeguards in both processes. Section 6.5 discusses the challenges that the imbalance in aim, functions and safeguards between the two regimes – national security and criminal law enforcement – poses for evidence gathering in criminal investigations. Section 6.6 concludes by suggesting implementing appropriate safeguards for data sharing mechanisms between the two regimes.

⁶ Jacqueline E. Ross and Stephen C. Thaman, 'Introduction: Mapping Dialogue and Change in Comparative Criminal Procedure', in Jacqueline Ross and Stephen Thaman (eds.), *Comparative Criminal Procedure* (Cheltenham: Edward Elgar, 2016), 27–28; John A. E. Vervaele, 'Special Procedural Measures and the Protection of Human Rights: General Report' (2009) 80(1) *Revue Internationale de Droit Pénal* [*International Review of Penal Law*] 75–123.

⁷ Roach, 'The Eroding Distinction', 48–68; UN General Assembly, 'Report of the Special Rapporteur', 13–19.

⁸ Tatiana Tropina, 'Comparative Report', in Ulrich Sieber, Nicolas von zur Mühlen and Tatiana Tropina (eds.), *Access to Telecommunication Data in Criminal Justice: A Comparative Analysis*, 2nd ed. (Berlin: Duncker & Humblot, 2021), 15–16.

6.2 NATIONAL SECURITY AND CRIMINAL JUSTICE: DEMARCATION

The root of the problem of information exchange between intelligence agencies and law enforcement lies in the fundamentally different functions of the national security and criminal justice regimes, their different focus and objectives. A line between the two can be drawn concerning not only the differences in their mandates – security of state and criminal justice – but also the *raisons d'être* of these domains. The demarcation lies in the nature of the societal dangers these two regimes are tasked with addressing.

The ultimate aim of the law enforcement agencies in the context of criminal justice is to investigate a crime that has already happened, identify the suspect and collect information as evidence to attribute the crime to that particular person. The ultimate aim of this process, which should strictly follow the steps outlined in the criminal procedure and is a subject – at least in democratic countries – of various safeguards and judicial oversight, is to build a case and bring perpetrators to justice. At the core of this traditional approach to criminal law enforcement is the collection of information about crime and suspects *post delictum*. This information gathering related to the investigation (as opposed to prevention) of crime is always reactive and aims at bringing evidence to the court.

In contrast to criminal investigations and the work of law enforcement in the domain of criminal justice, the objectives and functions of the intelligence agencies, which collect and analyse information for the purpose of national security, are more proactive and forward-looking. These agencies are tasked with protecting the state's security in a way that recognises current and future threats to the legal and political order with a primary aim to mitigate these risks and prevent them.⁹ In criminal investigations, the goal and the end of the data collection process is a criminal trial; however, such clear demarcation as to when the data collection ends in terms of data losing its relevance is absent in the process of information gathering by the national security agencies.¹⁰

Brodeur,¹¹ who calls surveillance by national security agencies 'high policing' and surveillance by law enforcement for criminal investigations 'low policing', demarcates these two types of 'policing' based on the expectation of whether the collection of data will result in action. 'High policing' by the intelligence agencies with the aim to protect the state can result in action only in the absence of other alternatives. In contrast, the work of law enforcement agencies, 'low policing', is supposed to culminate in action in the form of a criminal trial.¹²

The reactivity of law enforcement, as opposed to the proactivity of national security agencies, together with the notion of data collection for crime investigation resulting in action (trial) define the differences in *modus operandi* of these two regimes. Tied to its ultimate aim of attributing the criminal act to a particular person, the value of criminal procedures lies primarily in crime control achieved via due process that allows for an open examination of collected

⁹ James Waldo, Herbert S. Lin and Lynette I. Millett (eds.), *Engaging Privacy and Information Technology in a Digital Age* (Washington, DC: National Academies Press, 2007), 277; John A. E. Vervaele, 'Terrorism and Information Sharing between the Intelligence and Law Enforcement Communities in the US and the Netherlands: Emergency Criminal Law?' (2005) 76(3) *Revue internationale de droit pénal* 413; Permanent Select Committee on Intelligence House of Representatives, 'One Hundred Fourth Congress. IC21: The Intelligence Community in the 21st Century. Staff Study', 5 June 1996, www.govinfo.gov/app/details/GPO-IC21/summary; Diego Esparza and Thomas C. Bruneau, 'Closing the Gap between Law Enforcement and National Security Intelligence: Comparative Approaches' (2019) 32(2) *International Journal of Intelligence and CounterIntelligence* 322–353.

¹⁰ Ross and Thaman, 'Introduction: Mapping Dialogue and Change', 28–29.

¹¹ Jean-Paul Brodeur, 'High and Low Policing in Post-9/11 Times' (2007) 1(1) *Policing: A Journal of Policy and Practice* 25–37.

¹² *Ibid.*, 26–27.

evidence in a fair trial. In contrast, the value of the outputs produced by intelligence agencies is mainly achieved via collecting secret information that enables various government agencies to make better decisions in addressing threats to national security.¹³ While the law enforcement agencies in criminal investigations also covertly collect data in criminal investigations, the purpose of this process – criminal trial – means that this collection can later be challenged by the open examination. In contrast, secrecy is at the very core of the tasks of the national security agencies.

This distinction between the functions of law enforcement and those of national security defined the logic of their strict separation in the aftermath of the Second World War when experiences with totalitarian political regimes raised concerns about political control over criminal law enforcement.¹⁴ As Manget metaphorically describes it, ‘in the beginning there was the wall’,¹⁵ a strict separation between the tasks and the structures responsible for the security of the state and criminal justice, which prevented information sharing between the police and the national security agencies. This separation was respected in democratic societies until the complexity of challenges related to the threat landscape drove the two distinct regimes closer to each other, shifting the focus from reaction to prevention and increasingly leading to the securitisation of law enforcement and criminal justice.¹⁶

6.3 THE SHIFT IN PARADIGM: THE BLURRING LINES BETWEEN NATIONAL SECURITY AND CRIMINAL JUSTICE

While the paradigm shift can be significantly attributed to such turning points as the major terrorist attacks, particularly the 9/11 attacks in the USA,¹⁷ the trend can be traced to a much earlier time. More than a decade before the tragic events that happened in the USA in September 2001, Jakobs¹⁸ warned in 1985 about the rise of the concept of ‘enemy criminal law’ (*Feindstrafrecht*), which referred to certain types of criminals, such as terrorists, as the enemies of society whose criminal action denies the society’s legal order in its entirety. This concept was contrasted with ‘citizens criminal law’ (*Bürgerstrafrecht*), where the function of criminal justice lay in repairing the damage caused by the offence while still accepting the offender as a citizen. The rise of the ‘enemy criminal law’ was considered by the author of this concept a problematic development, which could be warranted only in a state of emergency.¹⁹ This concept corresponds to trends witnessed in criminal law enforcement in the aftermath of the 9/11 attacks when many states increasingly consider certain types of offenders, such as terrorists, not only as criminals but also as threats to national security and social order. The growing notion that certain types of offences also represent a threat to national security puts organised crime,

¹³ Roach, ‘The Eroding Distinction’, 49–51.

¹⁴ Vervaele, ‘Terrorism and Information Sharing’, 413.

¹⁵ Fred F. Manget, ‘Intelligence and the Criminal Law System’ (2006) 17 *Stanford Law and Policy Review* 416.

¹⁶ Valsamis Mitsilegas, ‘The Preventive Turn in European Security Policy: Towards a Rule of Law Crisis?’, in Francesca Bignami (ed.), *EU Law in Populist Times: Crises and Prospects* (Cambridge: Cambridge University Press, 2020), 301–302.

¹⁷ Nurse, ‘The Citizen and the State’, 6; Paul De Hert, ‘Balancing Security and Liberty within the European Human Rights Framework: A Critical Reading of the Court’s Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11’ (2005) 1(1) *Utrecht Law Review* 68; Vervaele, ‘Terrorism and Information Sharing’, 409–410.

¹⁸ Günther Jakobs, ‘Kriminalisierung im Vorfeld einer Rechtsgutsverletzung’ (1985) 97(4) *Zeitschrift für die gesamte Strafrechtswissenschaft* 751–785.

¹⁹ Günther Jakobs, ‘Bürgerstrafrecht und Feindstrafrecht’ (2004) 21 *Ritsumeikan Law Review* 93–107; Felix Golser, ‘The Concept of a Special Criminal Law as a Weapon Against “Enemies” of the Society’ (2016) 67 *Studia Iuridica* 65–77.

terrorism, attacks against critical infrastructures and large-scale ransomware incidents into the domain of both criminal justice and intelligence agencies.²⁰ The two previously very distinct regimes are expanding their functions related to the protection of society from threats, and this expansion changes their nature and blurs the borders between them. As a result, national security agencies and law enforcement have undergone various transformations concerning their role and functions.

The changing notion of what should be considered a threat to the state has a significant impact on the functions of both law enforcement bodies and national security agencies.²¹ On the one hand, the need to collect and analyse information about the dangers that can be considered both a crime and a threat to national security places the intelligence communities outside of their traditional mandate and sees them ‘gaining ground in the criminal justice system’.²² On the other hand, even more dramatic and fundamental changes can be witnessed in the nature and functions of the law enforcement agencies. The evolving landscape of complex threats increasingly pressures traditional criminal law enforcement to move from addressing the violation of public order *ex post* in a ‘prosecution-directed mode’²³ to focus on the identification of risks and disruption and mitigation of criminal activity,²⁴ from reaction to prevention. As noted by Koops, the ‘footprint of criminal law is becoming larger and larger’²⁵ via the expansion of substantive law and the criminal procedure frameworks that goes along with significant changes in the architecture of society. The latter also concerns technological changes: the focus is moving from reaction to prevention due to the availability of a considerable volume of digital data that can help detect and investigate crimes.

Data retention obligations imposed on communication providers in Europe and elsewhere are a good example of the shifting paradigms and blurring borders between national security and criminal investigations regimes. As opposed to targeted retention of data in the course of investigation of a particular crime, bulk retention of data represents a fundamental change of approach to evidence from the traditional paradigm where law enforcement had to actively search for sources of evidence to reshaping societal architectures in a way that presumably makes evidence readily available.²⁶ Retention frameworks impose obligations on communications providers to collect and store data of users of communication services regardless of any particular crime and in the absence of any suspicion. Even though these frameworks aim to preserve data that identifies communication, such as information about communication, and does not concern its content, the scope of data collected for retention can be extensive: from information about its duration to data about equipment used. While developed as purely preventive measures to address the challenges of serious crime and terrorism, data retention obligations are a perfect

²⁰ Vervaele, ‘Terrorism and Information Sharing’, 410; Nurse, ‘The Citizen and the State’, 6; Joyce Hakmeh and Kerstin Vignard, ‘ICTs, International Security, and Cybercrime’, UNIDIR, 11 October 2021, 12, www.unidir.org/publication/icts-international-security-and-cybercrime.

²¹ Hartmut Aden, ‘Information Sharing, Secrecy and Trust among Law Enforcement and Secret Service Institutions in the European Union’ (2018) 41(4) *West European Politics* 990.

²² Vervaele, ‘Special Procedural Measures’, 88.

²³ Martin Innes and James W. E. Sheptycki, ‘From Detection to Disruption’ (2004) 14(1) *International Criminal Justice Review* 1.

²⁴ David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 2nd ed. (USA: Books Express, 2009), <https://portal.cops.usdoj.gov/resourcecenter/content.ashx/cops-po64-pub.pdf>; Innes and Sheptycki, ‘From Detection to Disruption’, 2; Michael Price, ‘National Security and Local Police’, Brennan Center, 10 December 2013, www.brennancenter.org/our-work/research-reports/national-security-and-local-police.

²⁵ Bert-Jaap Koops, ‘Technology and the Crime Society: Rethinking Legal Protection’ (2009) 1(1) *Law, Innovation & Technology* 9.

²⁶ *Ibid.*, 15.

illustration of a cross-domain approach: law enforcement and national security agencies benefit from retained data alike.²⁷

The shift in paradigm and cross-domain approaches has changed the perception of the preventive role of criminal law and criminal justice. Undeniably, criminal law has always been expected to bear a strong preventive function.²⁸ By prohibiting certain types of unwanted behaviour as an *ultima ratio* response to societal dangers under the threat of punishment, criminal law aims to prevent them.²⁹ However, the core function of criminal procedure and law enforcement has been traditionally reactive and sought to punish those guilty of violating the legal order by committing offences. Enforcement of criminal law for this purpose follows a step-by-step order of action prescribed by the criminal procedure: identification of suspects, collection of evidence and, ultimately, a trial. In contrast to this traditional approach, the past two decades have witnessed the rise of the concepts of preventive policing and crime disruption at the early stages, gradually introducing more active preventive functions of the law enforcement agencies.³⁰

However, the development of more proactive approaches to crime control has not eliminated the classic paradigm. The two functions of criminal law enforcement coexist,³¹ with the new proactive function gaining more prominence and expanding beyond terrorism and organised crime to many other forms of predatory crimes.³² While the remainder of this chapter focuses on data collection by law enforcement for the purpose of criminal investigation, the complexity of the coexistence of preventive and reactive functions attributed to the law enforcement authorities should be highlighted as one of the factors contributing to the increasing complexity of regimes of data collection. Law enforcement agencies increasingly engage in the collection of data outside of criminal investigation for preventive purposes. When the mandate of the law enforcement agencies is gradually expanding from reacting to criminal acts to prevention, this expansion makes it difficult to draw a clear line between the law enforcement agencies and the national security actors. This shift from reaction to prevention has brought the law enforcement bodies even closer to the national security agencies, which always have proactive approaches at the core of their mandate.

Acknowledging that the borders between national security and criminal law enforcement are increasingly blurred with the growing importance of the preventive function of law enforcement agencies, the rest of this chapter distinguishes the two domains in the context of evidence gathering in criminal procedure. In this context, a clearer line can be drawn based on the

²⁷ International Association of Chiefs of Police (IACP), *Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence*, 2019, 8, www.theiacp.org/sites/default/files/2019-05/IACPSummitReportGoingDark_o.pdf; Michael Vincent Hayden, *Playing to the Edge: American Intelligence in the Age of Terror* (New York: Penguin Press, 2016), 83.

²⁸ Andrew Ashworth and Lucia Zedner, 'Punishment Paradigms and the Role of the Preventive State', in A. P. Simester, Antje Du Bois-pedain and Ulfrid Neumann (eds.), *Liberal Criminal Theory: Essays for Andreas von Hirsch* (Oxford: Bloomsbury, 2016), 3.

²⁹ Andrew Ashworth and Lucia Zedner, 'Prevention and Criminalization: Justifications and Limits' (2012) 15(4) *New Criminal Law Review: An International and Interdisciplinary Journal* 543; Johs Andenaes, 'General Prevention: Illusion or Reality?' (1952) 43(2) *Journal of Criminal Law, Criminology, and Police Science* 176–198.

³⁰ Nurse, 'The Citizen and the State', 6; Mitsilegas, 'The Preventive Turn', 301–302.

³¹ Ivan Škorvánek, Bert-Jaap Koops and Tjerk Timan, 'Surveillance, Criminal Procedure, and Regulatory Connection: The Case of Sewage Monitoring' (2019) 4 *TILT Law & Technology Working Paper*, 8, www.tilburguniversity.edu/sites/default/files/download/DP2019-004.pdf.

³² David L. Carter, *Law Enforcement Intelligence Analysis and Crime Analysis: Understanding Their differences and Cooperative Value*, Intelligence Policy Paper, September 2015, 6–7, www.researchgate.net/publication/282293348_LAW_ENFORCEMENT_INTELLIGENCE_ANALYSIS_AND_CRIME_ANALYSIS_UNDERSTANDING_THEIR_DIFFERENCES_AND_COOPERATIVE_VALUE/references.

fundamental nature of evidence collection in crime investigations: criminal procedure and criminal trial cannot be performed in relation to acts that are not committed yet. The approach to crime investigation is always reactive: the purpose of the evidence collection is to identify the person guilty in the criminal act that has already taken place³³ and prove the link between the criminal act and the suspect after the act has been committed. In contrast, data collection for the purpose of national security is driven by a preventive logic and can be performed in the absence of a crime, in the absence of a particular suspect or even in the absence of suspicion.³⁴ This major difference poses numerous challenges when law enforcement receives data from national security agencies and uses it in criminal investigations.

6.4 NATIONAL SECURITY, CRIMINAL LAW ENFORCEMENT AND DATA COLLECTION: DIFFERENCES IN SAFEGUARDS

The frameworks for collection of evidence with the purpose of linking the criminal act to a suspect can significantly vary depending on the criminal procedural law in the national jurisdiction in terms of investigative frameworks, regimes of authorisation and safeguards.³⁵ Yet the concept and the logic of crime investigation stay the same: the criminal procedure is an evidence-based *ex post* process. In contrast, while the concept of ‘national security’ and its interpretations can vary significantly,³⁶ at its very core the data collection for this purpose bears a preventive function. While there is a diversity of national frameworks that enable data collection by national security agencies, due to the differences between reactive and preventive objectives, most of the traditional practices of data collection for national security purposes fundamentally differ from the methods in criminal procedure in their nature, goals and safeguards.

These differences do not pose a problem per se when the two domains are strictly separated, with information flows between them strictly limited. Yet when national security agencies and law enforcement actors get closer to each other and cooperate in addressing the same complex threats, the exchange of data collected under these two regimes becomes problematic for criminal justice. As further discussed in this chapter, the difficulties arise from an imbalance between strict safeguards established for collecting evidence in criminal procedure and fewer protections in the data gathering for the purpose of national security. The most problematic aspects of this data exchange are divergencies in the necessity and proportionality requirements, the role of suspicion in data gathering and the differences in authorisation and oversight.

6.4.1 Necessity and Proportionality

The requirements for necessity and proportionality are the fundamental safeguards for protecting privacy in clandestine data collections, for the purposes of both national security and criminal procedure. To be in accordance with international human rights standards, communication surveillance powers ‘can only be justified as far as they are strictly necessary for achieving

³³ Ross and Thaman, ‘Introduction: Mapping Dialogue and Change’, 27.

³⁴ Barry Friedman and Cynthia Benin Stein, ‘Redefining What’s Reasonable: The Protections for Policing’ (2016) 84(2) *George Washington Law Review* 281–353; Thomas Linder, ‘Debating Surveillance: A Critical Analysis of the Post-Snowden Public Discourse’, in Elisa Orrù, Maria Grazia Porcedda and Sebastian Weydner-Volkman (eds.), *Rethinking Surveillance and Control* (Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 2017), 85–114; Ross and Thaman, ‘Introduction: Mapping Dialogue and Change’, 28–29.

³⁵ Tropina, ‘Comparative Report’, 61–79.

³⁶ David Baldwin, ‘The Concept of Security’ (1997) 23(1) *Review of International Studies* 5–26.

a legitimate aim and meet the proportionality requirement' and 'must be limited to preventing or investigating the most serious crimes or threats'.³⁷ These principles have been considered in the body of case law by the ECtHR regarding both criminal procedure and data collection for the purpose of national security.

In one of its first judgments on the matter of targeted interception in criminal procedure – *Klass v. Germany* – the ECtHR stated that 'secret surveillance and its implications are facts that the Court, albeit to its regret, has held to be necessary, in modern-day conditions in a democratic society, in the interests of national security and for the prevention of disorder or crime'.³⁸ Concerning mass surveillance for the purpose of national security, ECtHR jurisprudence also accepts the necessity of interference with privacy in a democratic society when it pursues a legitimate aim under the margin of appreciation. This necessity was recognised by several decisions concerning bulk data collection, such as *Weber and Saravia v. Germany*, where the ECtHR asserted that strategic monitoring of communications falls under the margin of appreciation of national authorities in choosing the best way to achieve legitimate aims.³⁹ In *Centrum för rättvisa v. Sweden*, while finding a violation of Article 8 of the European Convention on Human Rights (ECHR), the ECtHR reconfirmed its acceptance that 'bulk interception regimes did not per se fall outside the States' margin of appreciation' and 'the decision to operate a bulk interception regime in order to identify threats to national security or against essential national interests is one which continues to fall within this margin'.⁴⁰ Similarly, in its judgment on *Big Brother Watch and Others v. the United Kingdom*, while holding that there has been a violation of Articles 8 and 10 of the ECHR, the Court considered that the existence of a bulk interception regime does not constitute a breach of the human rights standards of the Convention.⁴¹

While ECtHR jurisprudence recognises the necessity of both regimes of data collection, it still, as Bachmaier Winter points out, 'systematically avoids'⁴² making judgments about the balance of interests and refers these balancing acts to national authorities to perform in the context of particular cases. This reluctance can be explained by the supranational nature of the ECtHR and the fact that the decisions about proportionality are taken by authorities for each individual case of interference and restrictions.⁴³ However, national approaches to proportionality can vary significantly. For example, to ensure the principle of proportionality in criminal procedure, countries limit interception of content data in transmission and access to stored content data by establishing minimum punishment thresholds for enabling authorisation of this measure or creating lists of certain crimes that can be subject to targeted monitoring of communications.⁴⁴

Furthermore, additional measures to ensure proportionality can be applicable for individual cases. As the ECtHR stated in *Zakharov v. Russia*, the proportionality test should include

³⁷ UN General Assembly, *The Right to Privacy in the Digital Age*, report of the United Nations High Commissioner for Human Rights, A/HRC/39/29, 3 August 2018, 11.

³⁸ *Klass and Others v. Germany*, Appl. No. 5029/7, 6 September 1978, para. 48.

³⁹ *Weber and Saravia v. Germany*, Appl. No. 54934/00, 29 June 2006, para. 106.

⁴⁰ *Centrum för rättvisa v. Sweden*, Appl. No. 35252/08, 25 May 2021, para. 254.

⁴¹ *Big Brother Watch and Others v. the United Kingdom*, Appl. No. 58170/13, 62322/14 and 24960/15, 25 May 2021, paras. 274–275.

⁴² Lorena Bachmaier Winter, 'Proportionality, Mass Surveillance and Criminal Investigation: The Strasbourg Court Facing Big Brother', in Emmanouil Billis, Nandor Knust and Jon Petter Rui (eds.), *Proportionality in Crime Control and Criminal Justice* (Oxford: Hart, 2021), 327.

⁴³ Jeremy McBride, 'Proportionality and the European Convention on Human Rights', in Evelyn Ellis (ed.), *Principle of Proportionality in the Laws of Europe* (Oxford: Hart, 1999), 23.

⁴⁴ Tropina, 'Comparative Report', 69–72.

‘verifying, for example, whether it is possible to achieve the aims by less restrictive means’.⁴⁵ In criminal procedure, such verification can be performed in each individual case when the measure is authorised or later when evidence is assessed in a criminal trial.⁴⁶ In the indiscriminate data gathering for the purpose of national security, these requirements cannot be applied in the same way as this regime bears a very different preventive rather than reactive function and the concept of bulk data collection does not match the notion of proportionality of interference in the individual cases, thus creating an inherent disparity in safeguards.

In the European Union, the CJEU tried to address this inherent disparity and preventive logic of indiscriminate data collection in several judgments concerning data retention and other data collection measures, such as the real-time collection of traffic data. The CJEU approach developed from outlawing blanket data retention as disproportionate in 2014 to reanimating retention of and access to various types of data based on legal interests. In its landmark decision in *Digital Rights Ireland*, which invalidated the EU Data Retention Directive, the CJEU applied the criteria of appropriateness and necessity to the Directive’s provisions. The Court held that while data retention can be an appropriate tool for achieving a legitimate aim (fight against serious crime, such as organised crime and terrorism),⁴⁷ the Directive went beyond what was necessary for achieving a legitimate aim because it did not clearly outline procedures and safeguards related to interference with privacy.⁴⁸ Three years later, in the *Tele2 and Watson* judgment, the Court ruled that the *Digital Rights Ireland* principles apply to national laws that implemented the Directive.⁴⁹

The later CJEU decisions on data retention and access to data tried to adopt a granular approach to data retention, where necessity and proportionality of interference are evaluated depending on the type of data. The *Privacy International* judgment considered data retention and transmission of traffic and location data to national security and intelligence agencies. In this ruling, the CJEU recognised the ‘importance of the objective of safeguarding national security’ in justifying interference with fundamental rights. Yet the Court found that the ‘national legislation requiring providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies through general and indiscriminate transmission exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society’.⁵⁰

However, in the *La Quadrature du Net* judgment, the CJEU tried to create nuanced criteria for the permissibility of indiscriminate data retention under the principle of proportionality. These criteria are based on two factors: the hierarchy of different public interest objectives and threats (safeguarding national security, combating serious crime and preventing serious threats or serious attacks on public security, combating crime and safeguarding public security) and different types of data. Concerning retention of traffic and location data, the CJEU, in the *La Quadrature du Net* case, ruled that general and indiscriminate retention of data ‘exceeds the limits of what is strictly necessary’ even to combat serious crime preventing serious threats to public security.⁵¹ The same ruling, based on a hierarchy of legitimate interests and types of data, considers preventive retention of internet protocol (IP) addresses and data relating to civil

⁴⁵ *Roman Zakharov v. Russia*, Appl. No. 47143/065, 25 May 2021, para. 260.

⁴⁶ Winter, ‘Proportionality, Mass Surveillance and Criminal Investigation’, 325–329.

⁴⁷ Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Others* [2014] EU:C:2014:238, paras. 44–45.

⁴⁸ *Digital Rights Ireland and Others*, paras. 61, 65, 69.

⁴⁹ Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others* [2016] EU:C:2016:970.

⁵⁰ Case C-623/17, *Privacy International* [2020] EU:C:2020:790, paras. 75 and 81.

⁵¹ Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others* [2020] EU:C:2020:791, para. 141.

identity and the expedited retention of traffic and location data to combat crime and safeguard public security to satisfy the requirements of necessity and proportionality.⁵² The CJEU also permitted the automated analysis of traffic and location data. While considering such interference to be particularly serious, the judgment held that the automatic analysis could meet the necessity and proportionality requirements when the state implements this measure only for a strictly limited period and only when facing a genuine and present or foreseeable serious threat to national security, including terrorism.⁵³

6.4.2 *The Role of Suspicion*

The role of suspicion in the data collection processes for the purpose of criminal investigation highlights the major difference between these two processes and creates irreconcilable divergencies between the two. Both regimes use data collection methods that interfere with the privacy of people or groups of people; both significantly rely on the opportunities that digital technology offers for clandestine data collection; and both aim at gathering sensitive information. A large amount of this data could be irrelevant to the purpose of the task, be it in criminal investigation or analysing national security threats.⁵⁴ The requirement for reasonable suspicion represents one of the most fundamental differences between data collection for the purpose of national security and as evidence in criminal investigations. For the latter, suspicion is one of the crucial concepts and safeguards, while for the former it plays little or no role.⁵⁵

Suspicion is the primary ground for enabling evidence collection in criminal investigations by law enforcement agencies. This especially concerns the most invasive investigative measures, such as surveillance of communications, which have to be targeted.⁵⁶ The ECtHR in *Iordachi and Others v. Moldova, Zakharov v. Russia, Liblik and others v. Estonia* held that the existence of reasonable suspicion is a necessary prerequisite for authorising surveillance of communications in criminal investigations.⁵⁷

In contrast, national security agencies can collect data in the absence of suspicion and even in the absence of a particular crime. While this approach does not exclude their ability to perform targeted surveillance, it is indiscriminate monitoring, the bulk collection of data and further analysis in the absence of suspicion that is at the core of the function of national security agencies. The primary aim of data gathering for the purpose of national security is to enable consumers of intelligence to make decisions based on the analysis of risks. There is no need to ground the data collection in suspicion as a prerequisite for allowing surveillance: the information can be gathered indiscriminately without targeting a particular person. In contrast to criminal procedure, this process is not case-driven but focuses on identifying patterns rather than being centred on the investigation of wrongdoing of certain suspects.⁵⁸ The use of bulk data collection through providers further amplifies the gradual confluence of targeted surveillance for the purpose of crime investigation and indiscriminate monitoring in the absence of

⁵² *La Quadrature du Net and Others*, paras. 157, 158.

⁵³ *Ibid.*, paras. 177, 178.

⁵⁴ Waldo, Lin and Millett, 'Engaging Privacy and Information Technology', 292.

⁵⁵ UN General Assembly, A/HRC/39/29, p. 10; Ross and Thaman, 'Introduction: Mapping Dialogue and Change', 28–29; Friedman and Benin Stein, 'Redefining What's Reasonable', 286–287.

⁵⁶ UN General Assembly, A/HRC/39/29, p. 11.

⁵⁷ *Iordachi and Others v. Moldova*, Appl. No. 25198/02, 19 September 2009; *Roman Zakharov v. Russia*; *Liblik and others v. Estonia*, Appl. No. 173/15, 181/15, 374/15, 383/15, 386/15 and 388/15, 7 October 2019.

⁵⁸ Ross and Thaman, 'Introduction: Mapping Dialogue and Change', p. 28.

suspicion.⁵⁹ The scale and the scope of criminal law enforcement activities are therefore transforming from significant but targeted intrusions into the private life of a suspect in the criminal case to ‘relatively minor intrusions into the lives of massive numbers of people, almost all of whom are assumed to be innocent’.⁶⁰

The CJEU tried to set the requirement for targeted interference in data retention judgment in *La Quadrature du Net and Others* without exploring the conceptual level of inapplicability of the notion of suspicion. The Court grounded its decision on the degree of interference with privacy, which serves as a benchmark for requiring the most intrusive data retention measures to be targeted. While asserting that general and indiscriminate retention of traffic and location data does not meet the requirements of necessity,⁶¹ the CJEU held that the law could allow targeted retention provided that it is limited to what is strictly necessary depending on ‘the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted’.⁶² This, according to CJEU, can include ‘persons who have been identified beforehand, in the course of the applicable national procedures and on the basis of objective evidence, as posing a threat to public or national security’.⁶³ The ruling also allows setting limits by using the geographical criterion for areas where an existing situation is ‘characterised by a high risk of preparation for or commission of serious criminal offences’.⁶⁴

In the same judgment, when considering the real-time collection of traffic and location data to combat terrorism, the CJEU, based on the intrusive nature of this measure, established stricter protection requirements based on suspicion. The ruling holds that this measure should concern only ‘persons with respect to whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities’. At the same time, anybody who falls outside of this category ‘may only be the subject of non-real-time access, which may occur, in accordance with the Court’s case-law, only in particular situations, such as those involving terrorist activities, and where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating terrorism’.⁶⁵

The ECtHR has taken a more conceptual approach to the differences in the purpose and method of data collection by the national security agencies, asserting that the requirement of suspicion cannot be applicable in the same way as it is to criminal investigations. The ECtHR elaborated on this inapplicability in *Big Brother Watch and Others v. the United Kingdom*, stating that ‘the requirement of “reasonable suspicion”, which can be found in the Court’s case-law on targeted interception in the context of criminal investigations is less germane in the bulk interception context, the purpose of which is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence’.⁶⁶ Instead, the ECtHR stated in the same judgment that domestic law should have clear grounds when such measures should be authorised. While legal clarity could serve as a safeguard against abuse of

⁵⁹ Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi and Amandine Scherrer, ‘National Programmes for Mass Surveillance of Personal Data in EU MS and Their Compatibility with EU Law’ (2013) 62 *Liberty and Security in Europe* 15.

⁶⁰ Ross and Thaman, ‘Introduction: Mapping Dialogue and Change’, 29.

⁶¹ *La Quadrature du Net and Others*, para. 141.

⁶² *Ibid.*, para. 147.

⁶³ *Ibid.*, para. 149.

⁶⁴ *Ibid.*, para. 150.

⁶⁵ *Ibid.*, para. 188.

⁶⁶ *Big Brother Watch and Others v. the United Kingdom*, para. 348.

indiscriminate interception, the differences in requirement for suspicion are inherent in terms of imbalance in the protection of human rights and the level of conditions that must be met to obtain the data.

6.4.3 *Independent Oversight*

The issue of oversight is one of the central problems of information sharing between law enforcement and national security agencies in a criminal investigation for the collection and presentation of evidence. Since data collection happens in both domains in a clandestine manner and without the ability of those subjected to surveillance to challenge the measure, it is essential to guarantee a high level of protection of individual rights by providing independent oversight. This oversight can be performed *ex ante*, in the form of authorisation of a particular form of data collection, and *ex post*, when supervision concerns the ongoing surveillance measure. The *ex post* oversight can be performed by a supervisory authority (e.g. judges controlling the interception of communications in criminal procedure or oversight bodies performing supervision of bulk data collection) or happen during a criminal trial, where evidence can be challenged. It can also include the review of data collection based on individual complaints.⁶⁷

6.4.3.1 *Ex ante Oversight*

While ECtHR and CJEU case law requires *ex ante* oversight for the most intrusive measures of data collection for both regimes – national security and criminal justice – there is no clarity on whether such control should be judicial or administrative and what kind of interference with privacy strictly requires judicial approval. The ECtHR affirmed in several decisions (*Zakharov v. Russia*, *Klass v. Germany*, *Big Brother Watch and Others v. the United Kingdom*, *Szabo and Vissy v. Hungary*, *Centrum för rättvisa v. Sweden*)⁶⁸ that the oversight should be entrusted to judicial authorities as it offers ‘the best guarantees of independence, impartiality and a proper procedure’.⁶⁹ However, the Court finds judicial oversight only ‘in principle desirable’⁷⁰ and does not consider it a requirement.

The CJEU case law also shows that the requirement for oversight does not necessarily mean judicial oversight. In the *Telez and Watson* judgment, the Court held that access to retained data, except in validly established urgent cases, should be ‘subject to a prior review carried out either by a court or by an independent administrative body’.⁷¹ Similar wording is used in the judgment in *La Quadrature du Net and Others* requiring *an ex ante* review of access to traffic data. However, the urgent requests were provided with no exemption: the Court held that for such requests ‘review must take place within a short time’.⁷² Furthermore, the *Prokuratuur* ruling establishes the requirement for non-judicial authorisation to be independent. The CJEU held

⁶⁷ Gianclaudio Malgieri and Paul de Hert, ‘European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards “Good Enough” Oversight, Preferably but Not Necessarily by Judges’, in David Gray and Stephen E. Henderson (eds.), *The Cambridge Handbook of Surveillance Law* (Cambridge: Cambridge University Press, 2017), 511–512.

⁶⁸ *Roman Zakharov v. Russia*; *Klass and Others v. Germany*; *Big Brother Watch and Others v. the United Kingdom*; *Szabo and Vissy v. Hungary*, Appl. No. 37138/14, 12 January 2016; *Centrum för rättvisa v. Sweden*.

⁶⁹ *Centrum för rättvisa v. Sweden*, para. 250.

⁷⁰ *Klass and Others v. Germany*, para. 56.

⁷¹ Joined Cases C-203/15 and C-698/15, *Telez Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others* [2016] ECLI:EU:C:2016:970, para. 120.

⁷² *La Quadrature du Net and Others*, para. 189.

that a public prosecutor in Estonia was not in a position to authorise access to retained traffic or location data because it could not provide the guarantees to reconcile the interests of investigations with the fundamental rights to privacy and personal data protection.⁷³

In practice, the regimes of authorisation of gathering information for two distinct purposes – national security and crime investigation – can vary significantly in terms of who performs *ex ante* oversight by approving a particular measure of data collection. In criminal investigations, access to evidence, especially to various types of data – content data, traffic data, subscriber data – is subject to various authorisations, which depend on the intrusiveness of a particular investigative measure and can range in national laws from a requirement for judicial oversight for real-time collection of content data to the need for a prosecutor's approval for less intrusive measures, such as access to traffic data⁷⁴ (as was considered in the *Prokuratuur* judgment of the CJEU). While the safeguards related to oversight can vary greatly depending on the national jurisdiction, in general, criminal procedures offer a certain degree of oversight in the process of collection of data, balancing intrusion into private life by employing these various mechanisms and degrees of authorisation. Traditionally, in criminal investigations, the most privacy-intrusive surveillance measures such as the interception of communications in transmission or access to stored content data are subject to judicial approval.⁷⁵

In contrast, approaches to *ex ante* authorisation of data collection for the purpose of national security are much more fragmented and have fewer safeguards. Data gathering for national security can still be subject to different authorisation requirements. However, even the most intrusive measures in some countries rely on executive orders issued by ministries, special courts or special oversight bodies instead of judicial warrants.⁷⁶ For example, in Germany, the national security agency – the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*) – is allowed to perform communication surveillance to prevent dangers to the free democratic order or to the existence and security of Germany and its states. In contrast to the power of interception of communication in criminal procedure, which always requires a judicial warrant (section 100a of the German Code of Criminal Procedure), the authorisation for interception by the Federal Office for the Protection of the Constitution is issued by the executive branch: the Federal Ministry of the Interior.⁷⁷ The Intelligence Act adopted in France in July 2015⁷⁸ in the aftermath of the Charlie Hebdo magazine attacks in Paris⁷⁹ allowed surveillance for the purpose of national security without a judicial order. Such surveillance became a subject of authorisation by the French prime minister, delivered upon a non-binding opinion of the National Commission of Control of the Intelligence Techniques.⁸⁰

Even if the requirement for a warrant for surveillance by national security agencies formally meets the condition of judicial authorisation, the form of this authorisation – for example, when

⁷³ Case C-746/18, *Prokuratuur* [2021] EU:C:2021:152, paras. 51, 52, 57.

⁷⁴ Tropina, 'Comparative Report', 61–65 and 95–102.

⁷⁵ UN General Assembly, A/HRC/23/40, p. 14.

⁷⁶ Bigo et al., 'National Programmes for Mass Surveillance', 25.

⁷⁷ Benjamin Vogel, Patrick Köppen and Thomas Wahl, 'Germany', in Ulrich Sieber, Nicolas von zur Mühlen and Tatiana Tropina (eds.), *Access to Telecommunication Data in Criminal Justice: A Comparative Analysis*, 2nd revised and expanded ed. (Berlin: Duncker & Humblot, 2021), 781.

⁷⁸ Loi n° 2015-912 du 24 juillet 2015 relative au renseignement (2015 Intelligence Act), 24 July 2015, *Journal officiel* 26 July 2015.

⁷⁹ Angelique Chrisafis, 'France Passes New Surveillance Law in Wake of Charlie Hebdo Attack', *Guardian*, 5 May 2015, [theguardian.com/world/2015/may/05/france-passes-new-surveillance-law-in-wake-of-charlie-hebdo-attack](https://www.theguardian.com/world/2015/may/05/france-passes-new-surveillance-law-in-wake-of-charlie-hebdo-attack).

⁸⁰ Estelle De Marco, 'France', in Ulrich Sieber, Nicolas von zur Mühlen and Tatiana Tropina (eds.), *Access to Telecommunication Data in Criminal Justice: A Comparative Analysis*, 2nd revised and expanded ed. (Berlin: Duncker & Humblot, 2021), 439.

it has to be carried out by special courts – can still raise concerns. For instance, the ECtHR in *Centrum för rättvisa v. Sweden* asserted that the requirement for the Foreign Intelligence Court to approve signal intelligence carried out by the intelligence agency FRA offers significant safeguards against abuse.⁸¹ However, this assessment was criticised for equating the formal existence of a judicial authorisation requirement with the actual restraint on abuse of surveillance practices by intelligence agencies.⁸² Judge Pinto de Albuquerque, in his concurring opinion, disputed the independence of the Foreign Intelligence Court and stressed that ‘with its concealed procedure and unappealable and secret decisions, the FIC [Foreign Intelligence Court] is not a court administering justice in the name of the Swedish people and accountable to it It serves one sole purpose: to whitewash the FRA’s choices, which in reality means the Government’s own surveillance policy choices.’⁸³

The incompatibility of authorisation regimes and oversight requirements becomes problematic when the same measures of data gathering, such as interception of the content of communications or access to stored content data that would require a court warrant in criminal investigations, are lawfully collected by national security agencies without judicial authorisation and then shared with law enforcement. Such sharing practices could potentially allow law enforcement agencies to bypass the higher bar of safeguards set by the criminal procedure law. The procedural law requirements can potentially be circumvented by resorting to a less burdensome process of gathering sensitive data by national security actors to later use them in criminal investigations without additional approval.

6.4.3.2 *Ex post* Oversight

The ongoing supervision of surveillance measures can differ significantly in the domains of criminal investigations and law enforcement. In criminal investigations, there are usually requirements for oversight of such ongoing measures as interception and other forms of data collection.⁸⁴ These measures are also complemented by the limitations of the validity of the warrants and the strict conditions for renewal of authorisations.⁸⁵ Data gathering for the purpose of national security in democratic countries is also subject to oversight. However, as observed by Malgieri and de Hert,⁸⁶ in practice, there is a tendency for criminal investigations to have a system of judicial overview, while surveillance for national security is mainly overseen by non-judicial authorities, like special agencies, ministers and parliamentary committees. Such oversight can raise a question about independence and effective remedies. For example, in *Centrum för rättvisa v. Sweden*, the ECtHR asserted that the body tasked with supervising and monitoring bulk surveillance activities in Sweden *post facto* does not guarantee objectivity. This supervisory body – the Inspectorate – was performing oversight of the activity of the surveillance agency and, at the same time, was tasked with the examination of individual complaints. This dual role, according to the ECtHR, ‘may generate conflicts of interest and, therefore, the temptation to overlook an omission or misconduct in order to avoid criticism or other consequences’.⁸⁷

⁸¹ *Centrum för rättvisa v. Sweden*.

In Swedish, FRA stands for Försvarets radioanstalt (National Defence Radio Establishment).

⁸² Mark Klamber, ‘Big Brother’s Little, More Dangerous Brother: *Centrum för Rättvisa v. Sweden*’, VerfBlog, 1 June 2021, verfassungsblog.de/raettvisa/.

⁸³ *Centrum för rättvisa v. Sweden*, Concurring opinion of Judge Pinto de Albuquerque, para. 23.

⁸⁴ Tropina, ‘Comparative Report’, 86–87.

⁸⁵ *Ibid.*, 80–84.

⁸⁶ Malgieri and de Hert, ‘European Human Rights, Criminal Surveillance, and Intelligence Surveillance’, 518.

⁸⁷ *Centrum för rättvisa v. Sweden*, para. 359.

The differences in the possibility of challenging the legitimacy of data collection in a trial are another crucial factor of imbalance between oversight in the two data collection regimes. The value of evidence collected by law enforcement agencies in criminal investigations for the purpose of trial and conviction is strongly tied to its admissibility because the focus of criminal justice lies in proving guilt by collecting evidence and presenting it in court. The latter means that the evidence should be relevant to a particular case and has to be gathered in a manner that will ensure its future admissibility in the adversarial trial,⁸⁸ where this information will be made public.⁸⁹ Therefore, in criminal procedure, there is a possibility to review and challenge the legitimacy of data collection in a criminal trial.⁹⁰

In contrast, data gathered by national security agencies are rarely tested and challenged in courts;⁹¹ ‘secret service surveillance usually remains secret even after it is finished’.⁹² They are not meant to be openly contested, as the value of this data primarily lies in its secrecy. This secrecy is also accepted in case law: for example, the ECtHR judgment *Centrum för rättvisa v. Sweden* recognises the ‘legitimate need for secrecy’ in performing mass surveillance, its regulation and oversight.⁹³ Due to the different purposes and functions of the national security agencies, the data gathered and analysed in this domain may never end up in trial. Sensitive data is amassed in an ongoing manner, without any relevance to suspicion and guilt and without the requirement to demonstrate the need for gathering this data. This information largely remains secret. Even if the process of gathering to a certain degree can be a subject of judicial authorisation and review, the safeguards primarily concern the operational side, the procedure of collection itself rather than how data is combined, processed and used further.⁹⁴ As the value of information collected by national security agencies in the traditional paradigm has no connection to the admissibility of evidence in criminal procedure, the incompatibility of the logic of data collection between two regimes becomes problematic when data flows from national security agencies to the law enforcement bodies in criminal investigations.

6.5 THE CHALLENGES OF THE CROSS-DOMAIN APPROACH

The main challenges of sharing data between the two domains for the purpose of criminal investigations are threefold. The first issue concerns collection of and access to data gathered under the frameworks that, by their nature, follow preventive logic and are the product of the ‘reaction–prevention’ paradigm shift, such as data retention. While these measures are supposed to benefit both regimes – national security and criminal justice – policymakers, law enforcement and courts are struggling with the preventive nature of these measures and the lack of nuanced safeguards that stems from this nature. The second challenge relates to the level of safeguards in the data-sharing practices between the national security agencies and law enforcement and the use of this data in criminal investigations. The imbalance in requirements for approval and oversight in the

⁸⁸ Roach, ‘The Eroding Distinction between Intelligence and Evidence’; Jimeno-Bulnes, ‘The Use of Intelligence Information in Criminal Procedure’.

⁸⁹ Waldo, Lin and Millett, ‘Engaging Privacy and Information Technology’, 292.

⁹⁰ Škorvák, Koops and Timan, ‘Surveillance, Criminal Procedure, and Regulatory Connection’, 10.

⁹¹ Ross and Thaman, ‘Introduction: Mapping Dialogue and Change’, 28–29.

⁹² Malgieri and de Hert, ‘European Human Rights, Criminal Surveillance, and Intelligence Surveillance’, 518.

⁹³ *Centrum för rättvisa v. Sweden*, paras. 236, 263.

⁹⁴ Ross and Thaman, ‘Introduction: Mapping Dialogue and Change’, 28–29.

process of data collection can potentially allow bypassing the strict requirements established in criminal procedure. Lastly, criminal investigations that rely mostly or only on information supplied by the national security agencies pose a challenge to a fair trial and other fundamental rights.

6.5.1 *Preventive Approaches to Data Collection: The Need for Clarity and More Nuanced Safeguards*

As previously highlighted in this chapter, data retention frameworks are the quintessence of the preventive approach in both regimes: national security and criminal justice. Driven by the preventive logic of data collection⁹⁵ and inheriting traditional lower levels of safeguards existing in the preventive paradigm, these frameworks have been frequently criticised for the lack of proportionality and for the highly contested assumption that retaining data would significantly facilitate the investigation of serious crimes. By invalidating the EU Data Retention Directive in *Digital Rights Ireland*, the CJEU rejected blanket data retention due to a lack of safeguards.⁹⁶ However, recent judgments are developing a set of requirements that aim at a more nuanced approach to protecting fundamental rights depending on the level of intrusion. These safeguards concern both national security and serious crime and are linked to the level of intrusion into privacy that retention of and access to various types of data entails. By setting out a more granular level of safeguards, the CJEU is apparently attempting to find the balance between the legitimate needs of law enforcement and the intelligence community and protections of privacy and other rights.

While confirming the irreconcilability of bulk mass surveillance for the purpose of national security without appropriate safeguards in the *Privacy International* judgment, in *Quadrature du Net* the ruling tried to reconcile the approach with its previous invalidation of the Data Retention Directive and other judgments outlawing blanket data retention.⁹⁷ Even though the decision was criticised for reanimating data retention from ‘the “walking dead”’,⁹⁸ it attempts to provide more clarity on safeguards required for bulk data collection. The judgment does so by establishing a hierarchy of legitimate public interest objectives, which can be used to justify the permissibility of retention of a particular type of data. National security is at the top of this hierarchy.⁹⁹ While taking a more granular approach and trying to balance interference with legitimate interests, the judgment still suffers from the lack of clarity: for example, one of the legitimate objectives refers to combating ‘serious crime’¹⁰⁰ – a term that can vary in national legal interpretations and has been long criticised as vague and lacking consistency and shared understanding.¹⁰¹ There is another – even more ambiguous – term, ‘serious risk to public security’,¹⁰² which justifies the targeted retention of traffic and location data. Since the *Quadrature du Net* judgment concerns both legitimate interests in national security and crime investigations, the lack of certainty can affect

⁹⁵ Koops, ‘Technology and the Crime Society’, 15.

⁹⁶ *Digital Rights Ireland and Others*.

⁹⁷ *La Quadrature du Net and Others*.

⁹⁸ Juraj Sajfert, ‘Bulk Data Interception/Retention Judgments of the CJEU – A Victory and a Defeat for Privacy’, European Law Blog, 26 October 2020, europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/.

⁹⁹ *La Quadrature du Net and Others*, para. 135.

¹⁰⁰ *Ibid.*, para. 136.

¹⁰¹ Letizia Paoli, An Adriaenssen, Victoria Greenfield and Mieke Conicx, ‘Exploring Definitions of Serious Crime in EU Policy Documents and Academic Publications: A Content Analysis and Policy Implications’ (2017) 23 *European Journal on Criminal Policy and Research* 269–85.

¹⁰² *La Quadrature du Net and Others*, para. 148.

safeguards and lead to arbitrary interpretations of the permissibility of surveillance and necessary safeguards in both domains. As they have always been lower than in criminal investigations, these interpretations can potentially strengthen privacy protection requirements for data collection by the national security authorities. However, for criminal procedure frameworks the lack of clarity might be underwhelming and not positive as a development.

6.5.2 Data from National Security Agencies as Evidence in Crime Investigations: *Imbalance in Safeguards*

Data sharing between national security agencies and law enforcement has always been possible: even during the times of strict separation and the existence of ‘walls’ between the two domains, there were still some information flows between them, even in the form of mere clues.¹⁰³ The possibility of information transfers greatly depends on the national security architecture: these architectures are always unique as they have been shaped by many factors, such as historical background, individual systems of constitutional protections and separation of powers, the criminal justice system, and they can vary from almost no sharing to free sharing or sharing under very well elaborated special protocols for data exchanges.¹⁰⁴

Considering significant possible differences in safeguards between the two domains, the flow of data from national security agencies to inform criminal investigations poses substantial challenges for criminal law enforcement, especially with the expansion of surveillance and bulk data collection techniques employed by the national security communities with fewer restrictions. As a result of inherent differences in the two systems and related safeguards, intelligence agencies operate under a lower threshold concerning the requirement for approval of surveillance¹⁰⁵ and oversight of ongoing data collection. They lawfully carry out activities and employ practices that could be considered unlawful if conducted by law enforcement agencies.¹⁰⁶

Even if states impose requirements for authorisation and oversight of indiscriminate data collection by national security agencies, these safeguards can usually be less strict than criminal procedures¹⁰⁷ and, therefore, create incompatibility in protections between the two regimes. This incompatibility is well illustrated in the judgment of the Czech Constitutional Court, which found that the use of evidence supplied by military intelligence agencies for the purposes of economic crime investigation violated the fundamental right to privacy.¹⁰⁸ As highlighted by Polčák and colleagues, even though interception for the purpose of national security in the Czech Republic is subject to judicial approval, this approval is subject to fewer safeguards and is easier to obtain.¹⁰⁹ The Czech Constitutional Court decision asserts that, due to this imbalance, ‘intelligence service interceptions do not reach the guaranteed quality[] which is required by the Code of Criminal Procedure’.¹¹⁰

¹⁰³ Tropina, ‘Comparative Report’, 21–24.

¹⁰⁴ Ibid., 19–24.

¹⁰⁵ UN General Assembly, A/HRC/23/40, pp. 14–15.

¹⁰⁶ Manget, ‘Intelligence and the Criminal Law System’, 429.

¹⁰⁷ UN General Assembly, A/HRC/23/40, pp. 14–15.

¹⁰⁸ *Ústavní soud České republiky* (Constitutional Court of the Czech Republic), 29 February 2008, No. I. ÚS 3038/07 – for details, see *Yearbook of the Constitutional Court of the Czech Republic*, 2016, 98, www.usoud.cz/fileadmin/user_upload/ustavni_soud_www/Rocenky/Ustavni_soud_Rocenka_EN_2016_nahled.pdf.

¹⁰⁹ Radim Polčák, Jakub Harašta, Pavel Loutocký, Jakub Míšek and Václav Stupka, ‘Czech Republic’, in Ulrich Sieber, Nicolas von zur Mühlen and Tatiana Tropina (eds.), *Access to Telecommunication Data in Criminal Justice: A Comparative Analysis*, 2nd ed. (Berlin: Duncker & Humblot, 2021), 439.

¹¹⁰ Constitutional Court of the Czech Republic, No. I. ÚS 3038/07; the translation of the court decision is quoted from Polčák et al., ‘Czech Republic’, 439.

The case illustrates how, without proper oversight from beginning to end, the growing overlap between the two data collection regimes creates an opportunity to bypass the strict safeguards established by criminal procedure law. There is a danger that instead of applying for various judicial authorisations to get access to data, law enforcement can potentially rely on information collected by intelligence in the interest of national security under a non-judicial warrant and with lesser oversight. Even if the safeguards for such data transfers are strengthened on the national level, the transnational character of many crimes and threats raises the question of data obtained by the national security services from their foreign counterparts and further shared with the law enforcement agencies for use in criminal procedure. The risk that intelligence agencies can engage in ‘privacy shopping’ and exploit loopholes in privacy protection regimes¹¹¹ amplifies the problem of bypassing strict safeguards of the criminal law, especially when the national security services are involved in cross-border data exchange.

The scale of this problem in a particular national context will depend on the extent of imbalance between safeguards for data collection in criminal procedure and safeguards established for national security agencies’ activities. However, most countries that allow information flows between two regimes have to address the challenges related to the fundamental differences between these domains. This includes problems related to the reactive nature of traditional criminal law enforcement as opposed to the proactive risk-based nature of prevention, the relevance of the data collection process to suspicion and guilt, the evidentiary purpose of the information collected and the possibility of bypassing the strict safeguards that evidence collection is subject to. Ultimately, the overarching problem of the cross-systemic approach is moving the ‘axis of criminal justice from the individual committing a criminal act’¹¹² towards prevention and mitigation. The concept of acquiring evidence as a process that is subject to strong checks and balances is being replaced by the more invasive collection and analysis of information subject to limited oversight, fewer safeguards and fewer accountability mechanisms.

6.5.3 *Criminal Procedure and the Challenge of Classified Evidence*

Information flows become even more problematic when law enforcement authorities rely on the presentation of information acquired by the national security agencies outside of safeguards governing criminal procedure or even before the start of a criminal investigation. The rules of fair trial require criminal procedures to be public,¹¹³ while frameworks regulating the collection of information by national security agencies are governed by secrecy. When the evidence collected by national security and intelligence agencies is used in a criminal trial, the defendant and other parties potentially have only limited access to reviewing it because of national security clauses and rules related to the protection of classified information; the national security and intelligence agencies can invoke various clauses to protect information they collected in secrecy and thus prevent the defendant and other parties gaining access to all of the evidence.¹¹⁴ This possibility depends on the national laws of criminal procedure, and the circumstances for the application of these rules greatly vary in national jurisdictions. However, with the blurring of

¹¹¹ Bigo et al., ‘National Programmes for Mass Surveillance’, 26.

¹¹² Ibid., 13.

¹¹³ Universal Declaration of Human Rights, Paris, 10 December 1948, 217 A (III), Article 10; International Covenant on Civil and Political Rights, New York, 16 December 1966, 2200A (XXI), Article 14.

¹¹⁴ Jimeno-Bulnes, ‘The Use of Intelligence Information in Criminal Procedure’, 178; Waldo, Lin and Millett, ‘Engaging Privacy and Information Technology’, 277; Didier Bigo, Sergio Carrera, Nicholas Hernanz and Amandine Scherrer, ‘National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges’ (2015) 78 *Liberty and Security in Europe* 1–3.

borders and the growing exchange of information between the two regimes, the presentation of information collected secretly and without the safeguards applicable to the criminal procedure can potentially become a challenge for fair trial and protection of fundamental rights that many countries will have to solve.

6.6 CONCLUSION

The domains of national security and criminal law enforcement have fundamental differences in their scope and goals. In recent years, the borders between the two domains blurred due to the need to address complex threats, such as organised crime and terrorism. There is an increasing preventive shift in criminal justice and a growing data sharing between the two regimes even though they are governed by fundamentally different frameworks. Due to their nature and functions, they have a substantial imbalance in safeguards related to data collection. While this imbalance raises various concerns about detrimental effects on safeguards in criminal procedure, it should be acknowledged that when the two regimes come together – on a positive side – there is some effect of strengthening requirements for fundamental rights protection in the domain of national security. This includes, for example, the imposition of stricter requirements for necessity, proportionality and oversight on the indiscriminate collection of and access to data by national security agencies. There is also continuous pressure to revise the practices of indiscriminate surveillance. These developments are especially significant in case law such as CJEU judgments on data retention and ECtHR rulings on mass surveillance.

However, despite some progress in strengthening safeguards in the national security domain, the increase in data sharing between the national security agencies and law enforcement raises a fundamental question of bypassing safeguards in the criminal procedure by using data collected in the domain of national security. There is a more significant danger of using the national security frameworks for data gathering as an alternative to collecting evidence under the rule of criminal procedure. While the imbalance between scrutiny, accountability and oversight in the two regimes is inherent, the problem cannot be solved only by establishing the same frameworks for authorisation or independent supervision for data collection in both domains. Due to the differences in the nature of the data collection and the functions and contexts of operations between national security and criminal procedure, the safeguards cannot be applied in the same way.

Notwithstanding these concerns, it is unrealistic to demand that data sharing between national security services and law enforcement be prohibited. Due to the growing complexity of the threat landscape, these two regimes can benefit from data sharing when it is done correctly, with proper safeguards and under clear procedures. Furthermore, it is unrealistic to expect that cross-domain data collection and sharing can be stopped: it is hard to operate in silos while addressing complex threats, and data exchange is inevitable. Yet the risks that this data exchange poses to safeguards in criminal procedure due to an imbalance in privacy protections should not be ignored.

To mitigate risks to criminal investigations posed by disparities in safeguards, there is a need to elevate the level of scrutiny in cases where data that can be used as evidence in criminal procedure is collected by national security services and shared with the law enforcement agencies as evidence in criminal investigations. Firstly, this should be done by strengthening the frameworks for proportionality and oversight of data collection by the national security services. Secondly, more robust safeguards should be implemented for information sharing between the two regimes, making the flow of data subject to additional scrutiny and providing

clear safeguards and strict conditions for using data obtained from national security agencies as evidence in criminal procedure. The main aim of setting these clear frameworks for data sharing for the purpose of criminal investigations should be to reduce the opportunity for law enforcement agencies to engage in forum shopping by choosing the less burdensome ways of data collection and obtaining data from national security bodies. Ultimately, reducing the possibility of such forum shopping will prevent the ultimate danger: gradual replacement of evidence collection in criminal procedure with alternative practices employed by national security agencies with an ongoing circumvention and disregard of strict safeguards implemented for evidence gathering in criminal procedure.

From Mutual Trust to the Gordian Knot of Notifications

The EU e-Evidence Regulation and Directive

Theodore Christakis

7.1 INTRODUCTION

The adoption of the E-Evidence Regulation was considered to be one of the most pressing legislative projects, seen as essential to enable law enforcement authorities all over the European Union (EU) to effectively investigate crimes. However, it took seven years since requesting that this project be considered¹ and more than five years since the European Commission (EC or Commission) put forward the legislative package concerning electronic evidence (E-Evidence) in criminal matters, for the legislative process to be finally concluded in June 2023. Strongly divergent views on almost everything except the commonly held view that there is a need to adopt this legislative passage have divided the two EU co-legislators, the Council of the European Union (Council) and the European Parliament (EP or Parliament), not to mention the EC: the initial project has been substantively amended by both the Council and the EP.

So what exactly happened to E-Evidence? What can explain the divergences and delays that have occurred, in spite of the fact that all parties have acknowledged the importance of the project? Well, E-Evidence has been very much ‘lost in notification’.² This project was initiated in order to provide an innovative legal framework that enables the unprecedented challenges that police and judicial authorities face in accessing electronic evidence to be addressed. Electronic evidence is essential in more than 85% of all criminal investigations,³ but is often found in other jurisdictions in which the service provider (for instance a cloud provider like AWS, Microsoft or Google, or a social media company like Meta) is established. Traditional mutual legal assistance (MLA) instruments, or new ones based on the principle of mutual recognition (such as the European Investigation Order, EIO),⁴ which depend on inter-state requests, are deemed to be cumbersome and time-consuming.

The E-Evidence package was therefore based on an entirely different philosophy and mechanism, permitting law enforcement authorities (LEAs) to request data that is pertinent to criminal investigations directly from service providers. E-Evidence therefore aims to create an ‘unprecedented EU-wide legal framework for *direct cooperation* between judicial authorities and

¹ The Council of the EU had already asked the Commission to consider this project in 2016.

² Theodore Christakis, ‘Lost in Notification? Protective Logic as Compared to Efficiency in the European Parliament’s E-Evidence Draft Report’, *Cross Border Data Forum*, 7 January 2020, www.crossborderdataforum.org/lost-in-notification-protective-logic-as-compared-to-efficiency-in-the-european-parliaments-e-evidence-draft-report/.

³ See Section 7.3.1.

⁴ For an excellent comparison between the EIO and the mechanisms of the E-Evidence legislative package, see Stanislaw Tosza, ‘All Evidence Is Equal, but Electronic Evidence Is More Equal Than Any Other: The Relationship between the European Investigation Order and the European Production Order’ (2020) 11(2) *New Journal of European Criminal Law* 161–183.

service providers in the field of criminal procedure’,⁵ without, in principle,⁶ involving a state other than the one issuing the order.

Such a system was founded, as we will see, on a kind of ‘absolute mutual trust’ among EU member states, based on the idea that the actions of the authorities of the issuing member state should be deemed sufficient and trustworthy by the other member states, and that it will no longer be possible to review such requests – as is the case in MLA mechanisms. However, this system of ‘absolute mutual trust’ was strongly challenged during the negotiations. Both the Council and the EP wished to introduce a notification system, whereby the issuing state would notify the other member state(s) involved, giving it/them the option of reviewing the requests of the issuing authority, in order to ensure that human rights are protected and that no abuse occurs. While the Council and the EP agreed about the need for a notification system, they strongly diverged on the extent, content and outcome of such a system: Which state(s) should be notified? What would the content of the review be? What outcomes are desired? Should we provide the reviewing state with grounds for refusal and, if so, which grounds? And how do we ensure that the notification mechanism will be able to exercise its protective function without hindering the effectiveness of the new ‘direct cooperation’ mechanism and bring us back to the philosophy (and problems) of the MLA mechanisms?

This is one of the reasons why there has been such a delay on E-Evidence. Yet, the ‘notification knot’ has not been the only obstacle to the negotiation process. The EC, the Council and the EP disagreed on several other issues, beginning with the very title of the legislative package (‘electronic evidence’ or ‘electronic information?’) and the legal instruments that it should contain, and moving on to important substantive issues such as how human rights will be protected, the role of service providers, how conflicts of law problems should be addressed, and which categories of data should be covered by the legislative package and the corresponding legal regime.

The objective of this chapter is to provide an overview of all these issues. Section 7.2 briefly outlines the pre-history of E-Evidence, the different stages of the negotiating process and the overall context against which these developments took place. Section 7.3 lays out the positions of the various actors on some of the most contentious issues discussed during the negotiations. Section 7.4 focuses on the issue of notification and presents the various proposals submitted by the EU institutions on this fundamental issue, as well as the final solution given by the Regulation, while assessing their potential protective function and their capacity to keep the E-Evidence package effective and attractive to LEAs.

7.2 A PROJECT CONSIDERED NECESSARY AND URGENT, BUT STUCK IN THE LEGISLATIVE PROCESS

This part of the chapter recalls the numerous reasons that led the EU to initiate the E-Evidence project, before briefly presenting the main mechanisms proposed by the Commission. It then explains the different stages of the complicated negotiation process and ends by briefly recalling the international context against which these developments have taken place.

⁵ Vanessa Franssen, ‘The European Commission’s E-Evidence Proposal: Toward an EU-Wide Obligation for Service Providers to Cooperate with Law Enforcement?’, *European Law Blog*, 12 October 2018, <https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement>, original emphasis.

⁶ Unless the service provider refuses to execute the order, in which case the issuing state will need to request that the ‘executing state’ cooperates with it, in order to enforce the order and compel the service provider to produce the data.

7.2.1 The Reasons That Compelled the EU to Initiate the E-Evidence Project

The reasons why the EU initiated the E-Evidence project are both diverse and numerous. However, the main rationale of this project is to respond to the important legal issues raised by the globalisation of criminal evidence.

The digitalisation of our lives and the widespread use of information and communication technologies (ICTs) have led to new challenges for LEAs and a profound change in the way they conduct their criminal investigations. The EC has noted that today ‘E-Evidence in any form is relevant in around 85% of total criminal investigations’.⁷ Indeed, in order to resolve all kinds of crimes, LEAs need to access subscriber data (in order to find out, for instance, who is hiding behind a social media account or an email address), traffic data (for instance, location data or data that permits the identification of the source and destination of communications) or content data (for instance, the content of an email account stored in a digital format by a cloud provider).

The problem, however, is that such evidence is increasingly located across territorial borders. Before the rise of cloud computing, criminal evidence was generally only available within the requesting country’s territorial jurisdiction. This is no longer the case. Today, the content of emails, social network posts and other data relevant to criminal investigations is often in the control of a service provider headquartered in a different country. The EC found in 2018 that ‘in almost two thirds (65%) of the investigations where e-evidence is relevant, a request to service providers across borders (based in another jurisdiction) is needed’, which means that ‘more than half of [all criminal] investigations involve a cross-border request to access [electronic] evidence’.⁸

This globalisation of criminal evidence,⁹ which leads to a disconnect between the territorial jurisdiction of states and the ways in which data moves and is held across national borders, poses significant challenges for LEAs. It drives historic change in the rules on how LEAs can gain access to communications and other records while respecting privacy and human rights. Most of the time, evidence is obtained via traditional cross-border mechanisms such as mutual legal assistance treaties (MLATs). However, these procedures are widely considered to be too slow and cumbersome, thus reducing the effectiveness of investigations and prosecutions. When asked, for instance, to identify the main problems encountered with MLA processes in relation to competent authorities in the US, EU judicial authorities reported almost unanimously (94.1 per cent) in a 2019 survey that the amount of time needed for MLA procedures was the most challenging issue.¹⁰

In order to find solutions to these problems, LEAs have developed mechanisms that involve voluntary cooperation as an alternative channel to judicial inter-state cooperation. Such voluntary cooperation mechanisms consist of sending requests to service providers that are established in another jurisdiction. The service provider is not *obliged* to respond under international law, but can reply directly to such requests on a voluntary basis, as long as the requests concern non-content data.

However, voluntary cooperation appears fragile from a legal point of view. The EC stressed, for instance, that voluntary direct cooperation in relation to non-content data ‘can be unreliable,

⁷ European Commission, Staff Working Document, Impact Assessment (accompanying the E-Evidence legislative package), [2018] SWD/2018/118(final), 17 April 2018, 14.

⁸ Ibid., 14.

⁹ See Theodore Christakis, Jen Daskal and Peter Swire, ‘The Globalization of Criminal Evidence’, *IAPP Privacy Tracker*, October 2018, <https://iapp.org/news/a/the-globalization-of-criminal-evidence/>.

¹⁰ See Europol, Eurojust and European Judicial Network, ‘SIRIUS EU Digital Evidence Situation Report’, 2nd Annual Report, 1 December 2020, 23.

may not ensure respect of the appropriate procedural safeguards, is only possible with a limited number of service providers which all apply different policies, is not transparent and lacks accountability'. It also noted that the resulting fragmentation 'may generate legal uncertainty, raise questions on the legality of prosecution as well as concerns on the protection of fundamental rights and procedural safeguards for the persons related to such requests'.¹¹

In order to respond to these challenges, a number of initiatives have been launched within the EU since 2015,¹² and in 2016, following an invitation by the Council, the EC undertook to propose solutions, including legislation if required. The E-Evidence legislative package was subsequently presented in April 2018.

7.2.2 *Basic Features of the Commission's Initial Proposals*

Composed of a 68-page draft Regulation (Commission's draft),¹³ a draft Directive¹⁴ and a 283-page impact assessment study,¹⁵ the E-Evidence legislative package aims to facilitate European LEAs' access to electronic evidence and streamline cooperation with service providers while providing a series of guarantees to protect the fundamental rights of individuals. It also seeks to provide an alternative to existing MLA tools by enabling LEAs in one member state to obtain stored data directly from online service providers located in or represented within a second member state.

The draft Directive intends to oblige European service providers that offer services in more than one member state as well as non-European service providers that are active in the EU market to appoint a legal representative in (at least) one member state. That representative must have the capacity to accept and comply with orders to produce evidence in criminal proceedings from LEAs in any member state and will therefore function as an EU-wide legal contact person for national competent authorities. As Vanessa Franssen has explained, with this Directive, the EC 'intends, on one hand, to help national authorities investigating and prosecuting criminal offences to apply and enforce the obligations service providers have under national law and, on the other hand, [to] avoid disparate national obligations for service providers considering that some Member States already require mandatory legal representation on their territory while others do not (yet)'.¹⁶

The draft Regulation refers to four categories of data, namely 'subscriber', 'access', 'transactional' and 'content' data (see Section 7.3.2). The Regulation sets out a comprehensive scheme to facilitate LEAs' access to these four categories of data through two new legal instruments: the European Production Order (EPO) and the European Preservation Order (EPrO). In the case of

¹¹ European Commission, Recommendation for a Council decision authorising the opening of negotiations in view of an agreement between the EU and the USA on cross-border access to electronic evidence for judicial cooperation in criminal matters, [2019] COM/2019/70 final, 5 February 2019. See also European Commission, 'Questions and Answers: Mandate for the EU-U.S. Cooperation on Electronic Evidence', 5 February 2019, https://ec.europa.eu/commission/presscorner/detail/en/memo_19_863.

¹² These initiatives are detailed in European Commission, Impact Assessment, 6–7.

¹³ European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, [2018] COM/2018/225 final – 2018/0108, 17 April 2018 (Commission's draft).

¹⁴ European Commission, Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, [2018] COM/2018/226 final – 2018/0107, 17 April 2018 (draft Directive).

¹⁵ European Commission, Impact Assessment.

¹⁶ Franssen, 'The E-Evidence Proposal'. For the important issue of how service providers are defined, see also Tosza, 'All Evidence Is Equal', 172–173.

an EPO, providers would be compelled to send the data directly to the issuing member state authorities (within ten days in normal cases, six hours in cases where there is an emergency), subject to certain limitations. Like the CLOUD Act (see Section 7.2.4), E-Evidence stipulates that the obligation to produce or preserve electronic evidence exists ‘regardless of the location of data’. This means that an EPO could target a person residing in another member state or in a third country and that the obligation on service providers to deliver the requested data exists even if the data is stored in another member state or in a third country. The scope of E-Evidence is limited to ‘stored’ data, which means that ‘it would not be possible to use an EPO or EPrO to compel a service provider to keep and produce future traffic and location data’.¹⁷

It is very important to emphasise that, in principle, an EPO shall only be addressed to a service provider when he is acting as a *data controller* under the General Data Protection Regulation (GDPR). As the EC explained:

In situations where the data sought is stored or processed as part of an infrastructure provided by a service provider to a company, typically in case of hosting or software services, the company itself should be the primary addressee of a request by the investigating authorities. This may require an EIO or MLA procedure where the company would not be a service provider covered by the scope of this Regulation. The service provider can only be addressed by a European Production Order if it would not be appropriate to address the request to the company, in particular where this would create a risk of jeopardising the investigation, for example where the company itself is under investigation.¹⁸

Regulation (EU) 2023/1543, of 12 July 2023, as finally published in the Official Journal (OJ), explains indeed that

[b]y way of exception, the European Production Order may be directly addressed to the service provider that stores or otherwise processes the data on behalf of the controller, where:

- (a) the controller cannot be identified despite reasonable efforts on the part of the issuing authority; or
- (b) addressing the controller might be detrimental to the investigation.¹⁹

Interestingly, also, the Commission’s initial draft provided service providers with a series of grounds for refusal, including if an EPO ‘manifestly violates the Charter of Fundamental Rights of the European Union’. As we will see in Section 7.3.6, a number of stakeholders and scholars reacted unfavourably to this, fearing that it could lead to a kind of ‘privatisation’ of law enforcement.

In any case, if a service provider refuses to execute an EPO or an EPrO, the Commission’s draft provides for an enforcement mechanism: the authority in an issuing state may transfer the order to a competent authority in the enforcing state (which is the state in which the service provider established its legal representative) who should recognise and enforce the order. The Commission’s draft gave, nonetheless, the enforcing state a series of grounds for refusal which were the same as those that can be used by the service provider.²⁰ Where there is an objection by a service provider, the enforcing authority has the final word about whether to compel the provider to execute the order or not (and the provider may be subject to sanctions).

¹⁷ Franssen, ‘The E-Evidence Proposal’.

¹⁸ Commission’s draft, 17.

¹⁹ Regulation (EU) 2023/1543 of the European Parliament and of the Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, [2023] OJ L191/118, 12 July 2023 Art. 5(6) (Regulation (EU) 2023/1543).

²⁰ Commission’s draft, Art. 14.

7.2.3 A Difficult and Long Negotiation Process

Following the proposals introduced by the EC in April 2018 (the Regulation's 'Commission's draft', as well as the 'draft Directive'), the EU legislative process was launched.²¹ Following the EC's proposals, the Council quickly organised a number of meetings. Despite difficult negotiations between EU member states, the Council succeeded in adopting, on 7 December 2018, its 'general approach' on E-Evidence²² (Council's draft). However, the adoption of this draft legislation led to a storm of reactions by non-governmental organisations (NGOs), industry, Members of the European Parliament (MEPs) and at least seven EU member states, which opposed the Council's draft.²³

Unlike the Council, the Parliament advanced very slowly. E-Evidence was assigned to the Civil Liberties, Justice and Home Affairs (LIBE) Committee, which appointed MEP Birgit Sippel as its rapporteur. The LIBE Committee produced several interesting working documents,²⁴ but it took until 8 November 2019 for Ms Sippel to finally release her Report on the E-Evidence draft Regulation (Sippel's Report).²⁵ This Report constituted a huge departure from both the Council's general approach and the Commission's initial proposal. Indeed, it presented no less than 267 amendments to the Commission's proposal, aiming to modify not only every single article in the Commission and the Council's drafts but also certain important mechanisms and pillars of these drafts.

Despite the fact that on this occasion the NGOs' and industry's first reactions were generally positive, Sippel's Report provoked a strong reaction from the Commission, which led to an unusual institutional confrontation within the EU. In particular, the Commission was accused of circulating a non-paper that was highly critical of Sippel's Report to a selective list of stakeholders and MEPs (but not to the E-Evidence Rapporteur herself), claiming that the amendments suggested by the rapporteur would have a major impact on the efficiency of E-Evidence (Commission's Non-paper).

It is against this background that various political groups introduced a total of no fewer than 841 amendments to the E-Evidence proposal.²⁶ After several meetings, a new compromise proposal came out of the LIBE Committee. On 7 December 2020, LIBE finally voted in favour

²¹ Non-EU law experts should be reminded here that the Council and the Parliament have to approve an identical text for the proposal to become law. If the texts adopted by the Council and the Parliament exhibit significant differences, inter-institutional negotiations must take place. These usually take the form of tripartite meetings (or a 'trilogue') between the Parliament, the Council and the Commission.

²² Council of the EU, Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters – General Approach, 15020/18, 30 November 2018.

²³ The Netherlands, for instance, denounced the Council's text for having been adopted 'too fast' and stated that it 'opened the way for abuse by EU countries that lack sufficient guarantees over the rule of law and fundamental rights'.

²⁴ For a brief presentation and links to these documents, see Thomas Wahl, 'Further Concerns of EP Against E-Evidence Legislative Proposal', *Eucri*m, 19 April 2019, <https://eucri.m.eu/news/additional-concerns-ep-regarding-e-evidence-legislative-proposal>.

²⁵ European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 'Draft Report on the proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters', Rapporteur: Birgit Sippel (COM(2018) 0225 – C8-0155/2018 – 2018/0108(COD)), 24 October 2019, www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html#_ftn1.

²⁶ European Parliament, Draft Report, Amendments 583–841 'European Production and Preservation Orders for electronic evidence in criminal matters', [2019] PE642.987v01-00, 2018/0108(COD) 11 December 2019, www.europa.eu/doceo/document/LIBE-AM-644870_EN.pdf.

of the compromise proposal on the E-Evidence package (EP's Draft).²⁷ The inter-institutional negotiations between the EP, the Council and the EC started in February 2021.

This 'trilogue' was very complicated, marked by substantial divergences of view between the Council and the EP, with each of them setting 'red lines' which the other institution was finding difficult to accept.²⁸ In June 2022 the EP and Council negotiators announced that they had 'reached a political agreement on core elements of a package'.²⁹ However, it took seven more months for a final compromise text (Trilogues text)³⁰ to be agreed by the European institutions in January 2023. This, in turn, cleared the way for the adoption of Regulation (EU) 2023/1543³¹ and Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (Directive 2023/1544)³² on 12 July 2023.

7.2.4 The International Context

The international backdrop from which the E-Evidence initiative has emerged cannot be ignored. The EC's draft was presented only a year after the beginning of negotiations on the adoption of a Second Additional Protocol³³ at the Council of Europe Convention on Cybercrime, the main international framework governing access to electronic evidence by public authorities. The Budapest Convention aims to harmonise national laws on cyber-related crime, support the investigation of these crimes and increase international cooperation around the fight against cybercrime.³⁴

As highlighted previously, the evolution of ICTs has brought new opportunities as well as challenges, in particular in terms of access to electronic evidence in criminal proceedings. In order to address these significant challenges, the Cybercrime Convention Committee created in 2012 a working group which transformed into the Cloud Evidence Group, which ultimately recommended the adoption of a treaty update in the form of

²⁷ European Parliament, Draft Legislative Resolution on the proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters (COM (2018)0225 – C8-0155/2018 – 2018/0108(COD)).

²⁸ See Presidency of the Council of the EU, Lettre du Conseil à Mme Sippel, 7106/22, 17 March 2022, <https://edri.org/wp-content/uploads/2022/04/sto7106.fr22.pdf>.

²⁹ See European Parliament, 'Electronic Evidence: Significant Progress on Package', press release, 26 June 2022, www.europarl.europa.eu/news/en/press-room/20220628IPR34002/electronic-evidence-significant-progress-on-package.

³⁰ Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings – Analysis of the final compromise text, 20 January 2023, <https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf> (Trilogues text). The content of this text was final, but some corrections/improvements took place and the numbers of the recitals and articles changed in the finalised text adopted in summer 2023.

³¹ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191/118, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1543>.

³² Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (Legal Representative's Directive) [2023] OJ L 191/181, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023L1544>.

³³ See Details of Treaty No. 224, Council of Europe, www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=224.

³⁴ It should also be noted that this serves as a limited MLAT when the countries involved in a request do not have an existing MLAT.

a Second Additional Protocol.³⁵ From September 2017 to May 2021, over ninety sessions of negotiations were held, leading to the adoption of the Second Additional Protocol to the Convention on enhanced cooperation and the disclosure of electronic evidence on 17 November 2021, which was opened for signature in May 2022.

Furthermore, understanding the E-Evidence project requires a consideration of the transatlantic context. The CLOUD Act,³⁶ passed by US Congress in March 2018, undoubtedly marks a major change in the way cross-border access to evidence is developed.

The first part of the CLOUD Act mooted the pending Supreme Court case of *United States v. Microsoft*. To briefly summarise, Microsoft argued that a US warrant had no legal force because the emails sought by the FBI were stored outside the US, in Ireland. The US argued that Microsoft could access the data from within the US and therefore the location in which the data happened to be stored did not matter. The CLOUD Act resolved this legal issue, providing that the kind of compelled disclosure orders at issue in the Microsoft Ireland case apply ‘regardless of whether such communication, record, or other information is located within or outside of the United States’.

The second part of the CLOUD Act created a new mechanism for other countries to access the content of communications held by US service providers. Under the Electronic Communications Privacy Act (ECPA),³⁷ US-based companies are prohibited from disclosing communications content directly to foreign governments. Foreign governments are instead required to make an MLAT or other diplomatic request for the data, even when it concerns the data of their own citizens in connection with local crime. This has been an increasing source of frustration for many governments, particularly since so much cloud-based data is held by US-based providers.

Nonetheless, the CLOUD Act enables these restrictions to be bypassed in specified circumstances, based on the adoption of ‘executive agreements’ between the US and other countries, and subject to a number of baseline substantive and procedural requirements. Where executive agreements are in place, the blocking provisions of the ECPA are partially lifted, and foreign LEAs can directly request communications content pertaining to non-US citizens and residents from US-based service providers.

The first such ‘CLOUD Act executive agreement’ was concluded between the US and the UK on 7 October 2019.³⁸ A second agreement was signed with Australia in December 2021; however, negotiations are ongoing between the US and Canada.³⁹

On 25 September 2019, the EU and the US officially started negotiations on a transatlantic agreement on cross-border access to electronic evidence for judicial cooperation in criminal matters. The objective of these complex negotiations⁴⁰ was to facilitate transatlantic access to

³⁵ See Jennifer Daskal and Debrae Kennedy, ‘Budapest Convention: What Is It and How Is It Being Updated?’, *Cross Border Data Forum*, 2 July 2020, www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/.

³⁶ Clarifying Lawful Overseas Use of Data Act of 2018, www.justice.gov/criminal-oia/cloud-act-resources.

³⁷ For more details, see Chapter 21 in this volume.

³⁸ See Theodore Christakis, ‘21 Thoughts and Questions about the UK/US CLOUD Act Agreement: (And an Explanation of How It Works – With Charts)’, *European Law Blog*, 17 October 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3469704; Jennifer Daskal and Peter Swire, ‘The UK-US CLOUD Act Agreement Is Finally Here, Creating New Safeguards’, *Lawfare Blog*, 8 October 2019, www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards. See also Chapter 20 in this volume.

³⁹ See US Department of Justice, ‘CLOUD Act Resources’, www.justice.gov/criminal-oia/cloud-act-resources.

⁴⁰ See Theodore Christakis and Fabien Terpan, ‘EU–US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options’ (2021) 11(2) *International Data Privacy Law* 81–106, <https://doi.org/10.1093/idpl/tpaa022>.

electronic evidence and avoid conflict of laws between the EU and the US. However, the EC and the Council emphasised several times that the EU–US Agreement could only be finalised and adopted after the adoption of E-Evidence. As a consequence of the difficulties and delays experienced during the adoption of E-Evidence, these important negotiations stalled for almost two years, but they finally resumed in 2023 after the emergence of the E-Evidence compromise between the Council and the EP.⁴¹

7.3 SOME OF THE MOST CONTENTIOUS ISSUES (OTHER THAN NOTIFICATION)

This section of the chapter will identify the main issues that caused divergences between the European institutions during the negotiation process – other than the highly contentious issue of notification, which is discussed in Section 7.4. Negotiators disagreed on . . . almost everything, from the title of the Regulation to the issue of whether a separate Directive is also necessary, passing through several issues related to the protection of human rights. In this section we will examine some of the major points of contention.

7.3.1 *E-Evidence or Electronic Information?*

First of all, the EU institutions did not even agree about the title of the Regulation and whether the terms E-Evidence/electronic evidence should be used. The Commission’s draft defined ‘electronic evidence’ as ‘evidence stored in electronic form by or on behalf of a service provider at the time of receipt of a production or preservation order certificate, consisting in stored subscriber data, access data, transactional data and content data’.⁴² While the Council was happy with this definition (and with the title of the Regulation proposed by the Commission), Sippel’s Report objected to the use of this term. Sippel noted that ‘the terminology chosen by the Commission – “electronic evidence” – could automatically imply that the data gathered is admissible as evidence in a criminal proceeding’.⁴³ As a result, she suggested replacing the term with ‘a more neutral terminology, namely “electronic information”’.⁴⁴

The EP accepted this proposal. It proposed to rename the title of the Regulation as follows: ‘European Production and Preservation Orders for electronic *information* in criminal *proceedings*’. And it defined the term ‘electronic information’ as meaning ‘subscriber data, traffic data, or content data lawfully stored by a service provider at the time of the issuing of a European Production or Preservation order, that is requested for the purpose of serving as evidence during the investigation, prosecution and court proceedings relating to a criminal offence in a Member State, in accordance with national law’. The idea of the EP was that the information requested by an EPO may, in several cases, not constitute ‘evidence’. During the trilogues, however, the EP withdrew this proposal allowing for the Regulation to maintain its initial name, as proposed by the Commission, referring to ‘electronic evidence’.

⁴¹ See US Department of Justice, ‘Justice Department and European Commission Announces Resumption of U.S. and EU Negotiations on Electronic Evidence in Criminal Investigations’, press release, 2 March 2023, www.justice.gov/opa/pr/justice-department-and-european-commission-announces-resumption-us-and-eu-negotiations.

⁴² Commission’s draft, Art. 2(6).

⁴³ Sippel’s Report, 147.

⁴⁴ Ibid.

7.3.2 *The Crucial Question of What Data Is Covered, and the Distinct Legal Regime*

Another important divergence between the different EU institutions concerned the categories of data covered and the legal regime that applies. The Commission's draft distinguished four categories of data: 'subscriber data', 'access data', 'transactional data' and 'content data'.⁴⁵ At first sight these four categories may come as a surprise. While 'subscriber data' and 'content data' are categories that had already been introduced in a number of instruments, such as the Budapest Convention,⁴⁶ the categories of 'access data' and 'transactional data' were new, while the classic category of 'traffic data' (also called 'metadata') did not appear in the draft. In fact, the Commission decided to divide the category of 'traffic data' into two categories: 'access data' and 'transactional data'.

The Commission explained that the three categories of 'subscriber data', 'access data' and 'transactional data' were all part of the broader category 'non-content data'.⁴⁷ However, the Commission explained that it was also 'appropriate to single out access data as a specific data category' and to distinguish it from transactional data. According to the Commission, access data was used 'to indicate the commencement and termination of a user access session to a service', while transactional data was 'generally pursued to obtain information about the contacts and whereabouts of the user and may be served to establish a profile of an individual concerned'. As a result, Article 2 of the Commission's draft proposed, beyond definitions of 'subscriber'⁴⁸ and 'content' data,⁴⁹ definitions on 'access'⁵⁰ and 'transactional'⁵¹ data.

The EC also considered that the sensitivity of the data varies. As stated by Vanessa Franssen, according to the EC, subscriber data and access data may be 'less sensitive in nature' than transactional and content data, 'justifying less stringent legal conditions for their production and a larger scope of application'.⁵²

Therefore, as far as the EC's draft is concerned, whereas an EPO concerning subscriber data or access data 'may be issued' by a judge, court, prosecutor or competent authority, the production of transactional and content data can be ordered *only* by a judicial authority.⁵³ Similarly, production of subscriber data or access data may be pursued for 'all criminal offences', while transactional data or content data may be pursued only for criminal offences that are punishable by a custodial sentence of a maximum of at least three years.⁵⁴

The Council's draft has accepted all these elements and distinctions. In sharp contrast, Sippel's Report introduced numerous amendments. First, the Report rejected the new data categories introduced by the Commission ('access' and 'transactional' data) and returned to what was presented as 'clear data categories (based on existing EU and national legislation and in line with CJEU [Court of Justice of the European Union] case law)', namely 'subscriber', 'traffic' and 'content' data.⁵⁵

Sippel's Report also provided for a higher threshold for issuing production orders. According to the Report, EPOs that require production of content or traffic data 'may only be issued for

⁴⁵ Commission's draft, Rec. (20).

⁴⁶ See Council of Europe, Convention on Cybercrime, ETS No. 185, 23 November 2001, Arts. 18 and 21.

⁴⁷ Commission's draft, p. 14 and Rec. (20).

⁴⁸ See *ibid.*, Art. 2(7).

⁴⁹ See *ibid.*, Art. 2(10).

⁵⁰ See *ibid.*, Art. 2(8).

⁵¹ See *ibid.*, Art. 2(9).

⁵² Franssen, 'The E-Evidence Proposal'.

⁵³ Commission's draft, Art. 4(1) and (2).

⁵⁴ *Ibid.*, Art. 5.

⁵⁵ Sippel's Report, 147.

criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 5 years'.⁵⁶ This was two years more than the threshold in the Commission's and the Council's drafts. The intention was that, for these categories of data, EPOs can be issued only for the most serious crimes. The EP's Report maintained the three categories of data proposed by Sippel's Report ('subscriber', 'traffic' and 'content' data), proposing new definitions for 'subscriber'⁵⁷ and 'traffic'⁵⁸ data.

With regard to the issuing authority for EPOs, the draft of the EP distinguished two regimes: on the one hand, EPOs for 'subscriber data' and '[internet protocol] IP addresses' may be issued by a judge, court, investigating judge, public prosecutor or any other competent authority; on the other hand, EPOs for 'traffic' and 'content' data may be issued by a judge, court, investigating judge or any other competent authority, but not a prosecutor.

Interestingly, however, the EP's compromise did not align with Sippel's draft on the higher threshold for issuing production orders, and returned to the initial three-years threshold proposed by the Commission. It was clear, as a matter of fact, that LEAs around Europe would have never accepted such a high threshold.

The compromise found on all this during the trilogues was the following: the Regulation maintains the three traditional categories of 'subscriber', 'traffic' and 'content data', but adds, immediately after 'subscriber data', a category named 'data requested for the sole purpose of identifying the user'.⁵⁹ Production of subscriber data and data requested for the sole purpose of identifying the user may be pursued for 'all criminal offences' and orders can be issued by both a judge and a prosecutor. In contrast, the production of traffic data (except data requested for the sole purpose of identifying the user) and content data can be ordered *only* by a judicial authority and may be pursued only for criminal offences that are punishable by a custodial sentence of a maximum of at least three years as well as for some offences specifically defined in the Regulation.⁶⁰

7.3.3 *Merging the Directive into the Regulation?*

A third major area of disagreement concerned whether the E-Evidence legislative package should include both a Regulation and a Directive, as proposed by both the EC and the Council, or only a Regulation, as proposed by the EP. Sippel's Report proposed merging the two instruments proposed by the Commission into a single instrument. The rapporteur advanced several arguments to justify this, including the concern that by introducing a separate Directive (which will oblige service providers to designate a legal representative in the Union), the Commission might have the hidden intention to 'also use it for other future instruments'. 'In that regard', argued the rapporteur, 'the proposed Directive overreaches its goal and raises serious issues with its legal basis, namely the Articles 53 and 62 TFEU [Treaty on the Functioning of the European Union]'.⁶¹

⁵⁶ Ibid., 71.

⁵⁷ See EP's draft, Art. 2(7).

⁵⁸ See *ibid.*, Art. 2(8).

⁵⁹ Art. 3(10) of the Regulation explains that this 'means IP addresses and, where necessary, the relevant source ports and time stamp (namely the date and time), or technical equivalents of these identifiers and related information, where requested by law enforcement authorities or by judicial authorities for the sole purpose of identifying the user in a specific criminal investigation'.

⁶⁰ See Regulation (EU) 2023/1543, Arts. 4 and 5.

⁶¹ Sippel's Report, 146.

The Commission strongly opposed the suggested suppression of the proposed Directive, considering that this would deprive the whole E-Evidence package of its added value, especially as far as third-country service providers are concerned. The Commission emphasised that the legal basis for the Regulation (Art. 82(1) TFEU) cannot be used to compel service providers from third states to designate a legal representative in the Union. As a result, a different legal instrument, with a different legal basis, is necessary.⁶²

Nonetheless, the EP followed Sippel's approach. The EP abandoned the proposed Directive in its draft and introduced in the Regulation, instead, a new Article 6a entitled 'Legal Representative'.

All these proposals by the Parliament were abandoned during the trilogues. As a result, the final E-Evidence legislative package includes, as initially suggested by the Commission, both the Regulation and a Directive on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings.

7.3.4 *Requirement to Use the Regulation Instead of Domestic Measures*

Another contentious issue concerned the question of whether, once the Regulation has been adopted, EU member states will still be able to use parallel and concurrent domestic procedures in order to compel the production of data by service providers established in other jurisdictions.⁶³ The Commission's and the Council's approaches have created uncertainty and raised the possibility of member states potentially resorting to using domestic measures in cross-border scenarios. Service providers have expressed the concern that, if the language is not clarified, the Commission's and the Council's approaches could create a back door, giving member states the opportunity to simply ignore the E-Evidence legislation altogether and use domestic measures instead, which could lead to fragmentation and conflicts of law. Furthermore, as Lani Cosette from Microsoft noted: 'Requiring authorities to use an EU measure, rather than a domestic one, means all users will enjoy the same protections across the EU, regardless of the Member State making the demand or where the provider is established or has its legal representative.'⁶⁴

The EP's draft tried to address this issue by proposing to introduce in Article 1 the following text: 'Authorities of the Member States shall not issue domestic orders with extraterritorial effects for the production or preservation of electronic information that could be requested on the basis of this Regulation.' However, the final compromise text did not introduce this sentence proposed by the EP. This means that the ambiguity about this issue might persist. The precedent of the Terrorist Content Regulation⁶⁵ might be somehow concerning in this respect: it seems that more than one year after its adoption not a single EU member state has used the central mechanism of removal orders provided for by the Regulation, preferring the use of national procedures instead.

⁶² Commission's Non-paper already mentioned.

⁶³ It should be made clear, however, that the E-Evidence Regulation does not apply if there are no cross-border data issues. As Article 1(1), para. 2 states: 'This Regulation is without prejudice to the powers of national authorities to address service providers established or represented on their territory in order for them to comply with national measures similar to those referred to in the first subparagraph.'

⁶⁴ Lani Cossette, 'The Commission's E-Evidence Initiative: Harmonising EU Rules on Access to Electronic Evidence', in Valsamis Mitsilegas and Niovi Vavoula (eds.), *Surveillance and Privacy in the Digital Age: European, Transatlantic, and Global Perspectives* (London: Bloomsbury, 2021), 79.

⁶⁵ Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, [2021] OJ L 172, 17 May 2021.

The context is different, but it highlights that when the EU mechanisms are put in place after a long period of negotiations, these mechanisms should take precedence over national mechanisms. It would be expected that EU member states use the E-Evidence Regulation and not domestic procedures in order to make such cross-border data requests when the Regulation enters into application on 18 August 2026.⁶⁶

7.3.5 Human Rights Protections

Protection of human rights is a major aspect of the project.⁶⁷ The term ‘fundamental rights’ appears twenty times in the Commission’s proposal, a number which is brought down to seventeen in the Council’s draft. While numbers are not always relevant, it is nonetheless interesting to note that Sippel’s Report mentions the term thirty-one times and the EP’s draft mentions it twenty-four times.

It is fairly logical that such an important Regulation, which authorises direct access to personal data, should, as the Council stated in its draft, take ‘due account of the impact of the measure on the fundamental rights of the person whose data are sought’.⁶⁸ However, the negotiations were marked by substantial divergences on these issues. The present section will allude to some of these.

7.3.5.1 Who Can Raise Human Rights Issues?

The Commission’s proposal and, to a much greater degree, the Council’s draft entrusted the responsibility of protecting human rights mainly to the issuing authority. Recital 46 of the Council’s draft clearly explains that ‘the responsibility to ensure the legality of the Order, in particular its necessity and proportionality, should lie with the issuing authority’.

However, it is questionable whether the issuing state would be sufficiently incentivised to effectively protect the human rights of persons residing *outside* its territory. Entrusting the protection of human rights solely to the issuing authority could create numerous practical difficulties, including difficulties around remedies and redress mechanisms.⁶⁹ In order to limit this problem, the Commission afforded service providers and, under certain conditions, the enforcing state the power to refuse to execute an EPO if it ‘manifestly violates the Charter of Fundamental Rights of the European Union or ... is manifestly abusive’. However, this power was removed by the Council. Furthermore, the notification mechanism in the Council’s draft contained serious limitations and did not afford the member state of residence or the executing state the practical ability to protect human rights, by means of opposing an EPO.

Sippel’s Report adopted a much more protective approach to these issues, entrusting the responsibility of protecting human rights to both the ‘issuing’ and the ‘executing’ states but also, to the extent that this is relevant, to the member state of residence (the ‘affected’ state). However, the concept of the affected state did not survive the efforts of the EP and the Council to reach a compromise. We will discuss all these issues in more detail in Section 7.4.

⁶⁶ According to Art. 28.

⁶⁷ As soon as the project was presented, First Vice President Frans Timmermans of the EC claimed that it aimed to put in place ‘unprecedented tools enabling the competent authorities not only to gather electronic evidence quickly, efficiently across borders but also ensuring robust safeguards for the rights and freedoms of all affected’.

⁶⁸ Council’s draft, Rec. (29).

⁶⁹ For instance, this means that a data subject not residing in the issuing state would need to travel there in order to exercise his/her right to an effective remedy in local courts.

The final Regulation nonetheless gives power to the *enforcing* state to protect human rights under two different mechanisms. First, in cases where it receives a notification by the issuing state under Article 8, the enforcing state ‘shall raise’, according to Article 12, ‘grounds for refusal’ when it considers that the execution of the order could endanger some specific rights mentioned there (especially freedom of press or freedom of expression) or, ‘in exceptional situations’, entail ‘a manifest breach of a relevant fundamental right as set out in Article 6 of the Treaty on European Union (TEU) and the Charter’. Second, in cases where there is no notification, but where the service provider refuses to execute an EPO and the issuing state requests the help of the enforcing state to oblige the provider to do so, the enforcing state has the possibility (‘may’) to deny the enforcement of the EPO on the basis of human rights considerations very much similar to the ones mentioned earlier.

7.3.5.2 Dual Criminality Principle (and the Idea of a List of Crimes)

Both the Commission’s proposal and the Council’s draft abandon the dual criminality principle that was one of the cornerstones of the mutual recognition system in EU criminal law. According to both texts, preservation orders, as well as production orders for subscriber and access data, could be issued for all criminal offences. Production orders for transactional and content data can be issued for all criminal offences punishable in the issuing state by a custodial sentence of at least three years. Therefore, the principle of dual criminality will no longer apply, which means that orders could be sent for offences that are not deemed to be criminal in the member states where the service provider is located.

As the LIBE Committee of the EU Parliament noted,

bearing in mind the limited amount of harmonization in criminal law between Member States regarding, on the one hand, the definition of crimes (e.g. definitions of rebellion against the state, limits to freedom of expression, abortion rights, etc.), as well as the respective national rules regarding investigations of these crimes, the proposal goes much further than the current mutual recognition system in EU criminal law.⁷⁰

The European Data Protection Board (EDPB) also called for the introduction in E-Evidence of the dual criminality principle, emphasising that this ‘would for instance prevent a State from requiring the help of another one to imprison someone for their political opinions if these opinions are not criminalised in the requested State or to prosecute someone for having aborted if this person is residing in another State where it is not illegal’.⁷¹ Another solution proposed by some member states was to introduce in E-Evidence a consensual list of serious crimes punishable in all member states and to only reserve EPO requests for investigations that concern such crimes.

Sippel’s Report suggested to provide due regard for dual criminality considerations. The EP’s draft followed her approach by providing that an EPO for traffic or content data ‘may be refused’ by the executing state on the basis of dual criminality considerations.⁷²

⁷⁰ European Parliament, Committee on Civil Liberties, Justice and Home Affairs, ‘Working Document on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters – Introduction and overall assessment of issues’ (2018/0108 (COD)), 7 December 2018, 6, www.europarl.europa.eu/doceo/document/LIBE-DT-631925_EN.pdf?redirect.

⁷¹ European Data Protection Board, Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b), 26 September 2018, 6, https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-232018-commission-proposals-european-production_en (EDPB Opinion 23/2018).

⁷² EP’s draft, Art. 10a(2).

Article 12(1)(d) of the final Regulation introduced the dual criminality principle as a ‘ground for refusal’ for the enforcing state in cases where it is notified under Article 8. By using the term ‘shall’ (instead of ‘may’) this article also indicates that there is a real obligation for the notified enforcing state to do so, unless the conduct for which the EPO has been issued concerns an offence found in the list of crimes of Annex IV.⁷³

7.3.5.3 Notice to Users

Another important element of the discussions concerned procedural rights guarantees that begin with the right of the person whose data is sought to be informed that he or she has been targeted by an EPO. The Council’s draft took a very strict approach to this by introducing a principle whereby service providers should per default *not* notify users. According to the Council, service providers should be obliged to ‘refrain from informing the person whose data is being sought’ unless they are ‘explicitly requested [to do so] by the issuing authority’.⁷⁴

In contrast, Sippel’s Report provided for default notification if it concerns people who have been targeted by orders issued under the Regulation (unless there is a non-disclosure order validated by a court, to avoid jeopardising the investigation at hand).⁷⁵ The EP’s draft followed this suggestion and also noted that ‘such an order shall be duly justified, specify the duration of the obligation of confidentiality and shall be subject to periodic review’.⁷⁶

The final Regulation considers that ‘informing the person whose data are requested is an essential element as regards data protection rights and defence rights, in that it enables effective review and judicial redress’. Thus, it requires that the issuing authority should, in principle, and with the above-mentioned exceptions, inform the person whose data is being requested without undue delay.⁷⁷

7.3.5.4 The *ne bis in idem* Principle

The Council’s draft introduced a recital according to which ‘a European Production Order should not be issued[] if the issuing Member State has indications that this would be contrary to the *ne bis in idem* principle’.⁷⁸ However, one may wonder how the issuing member state would find out that parallel criminal proceedings on the same matter are ongoing in another member state if there is no notification to any other member state.

Sippel’s Report suggested introducing strong protections around the *ne bis in idem* principle and the EP’s draft endorsed this by providing that the authority of the executing state ‘shall refuse’ an EPO where ‘the execution of the European Production Order would be contrary to the principle of *ne bis in idem*’.⁷⁹ Article 10a(1)(c) of the final Trilogues text introduced, indeed, violations of the *ne bis in idem* principle as a mandatory ‘ground for refusal’ for the enforcing state, but only in cases where it is notified under Article 7a.

⁷³ When one reads the list of offences in Annex IV, he/she remains with the impression that, normally, all these offences (including terrorism, trafficking in human beings, corruption etc.) are recognised as such in all EU member states, so the utility of introducing them as an exception to the dual criminality principle is not very clear.

⁷⁴ Council’s draft, Art. 11(1).

⁷⁵ Sippel’s Report, Amendment 164.

⁷⁶ EP’s draft, Arts. 11(1) and 11(1a).

⁷⁷ See Regulation (EU) 2023/1543, Rec. (67) and Art. 13.

⁷⁸ The legal principle of *ne bis in idem* restricts the possibility of a defendant being prosecuted repeatedly on the basis of the same offence, act or facts. Council’s draft, Rec. (12a).

⁷⁹ EP’s draft, Art. 10a(1)(b).

7.3.5.5 Remedies

Both the Commission's proposal and the Council's draft provided in Article 17 for 'effective remedies' for the person whose data is being sought. Significant problems remained, nonetheless.

Both texts emphasised in Article 17(3) that 'such right to an effective remedy *shall be exercised before a court in the issuing State* in accordance with its national law and shall include the possibility to challenge the legality of the measure, including its necessity and proportionality'.⁸⁰ This could be highly problematic if the affected person does not reside in this country⁸¹ and/or has little knowledge of the legal system of the issuing member state (and is not proficient in the official language of this state).

Sippel's Report addresses this issue and stresses the importance of effective legal remedies both in the issuing and in the executing state that are in accordance with national law and include the ability to challenge the legality of the order. The EP followed this approach.⁸² The Trilogues text remains, nonetheless, a little bit ambiguous in this regard by stating: 'The right to an effective remedy shall be exercised before a court *in the issuing State* in accordance with its national law and shall include the possibility to challenge the legality of the measure, including its necessity and proportionality, *without prejudice to the guarantees of fundamental rights in the enforcing State*.'⁸³

7.3.6 Role and Obligations of Service Providers

The nature and extent of the role and obligations of service providers is an issue that has been discussed extensively from the day that the Commission's draft was introduced until today. The most important issue concerns responsibility for protecting human rights and the corresponding power of service providers to challenge the legality of EPOs.

Under the Commission's proposal, service providers possessed a variety of options to challenge the legality of EPOs and/or refuse to execute an order in some cases. In particular, under the Commission's draft, the service provider had an obligation to inform the issuing authority whenever it could not comply with its obligations due to: (i) an incomplete EPO; (ii) the EPO containing manifest errors; (iii) or the EPO not containing sufficient information to execute it.⁸⁴ Similarly, the service provider could be unable to comply because of a 'de facto impossibility' (e.g. because the person whose data is being sought is not a customer).⁸⁵ These provisions have not created any particular problems and have been maintained by the Council and the EP.

The Commission's draft also stressed that the service provider may oppose the enforcement of an EPO if the EPO 'has not been issued or validated by an issuing authority'⁸⁶ or 'has not been issued for an offence provided for by the Regulation'.⁸⁷ While these provisions did not appear that controversial, the Council decided to remove them from its draft. Yet, the EP's draft

⁸⁰ Emphasis added.

⁸¹ If, for instance, the Greek authorities request the data of a Spanish person residing in Spain, this means that the only possible remedy for this Spanish person to challenge the legality of the EPO will be to travel to Greece and present his/her case before a Greek court.

⁸² EP's draft, Art. 17(3).

⁸³ Trilogues text, Art. 17(2), emphasis added.

⁸⁴ Commission's draft, Art. 9(3).

⁸⁵ Ibid., Art. 9(4).

⁸⁶ Ibid., Art. 14(4a).

⁸⁷ Ibid., Art. 14(4b).

reintroduced the ability for the service provider to react in accordance with these motives, while reserving the final decision about the execution to the authorities of the executing state.

Other provisions in the Commission's draft provoked a strong reaction. The EC proposed that the service provider may oppose the execution if it considers that the EPO 'manifestly violates the Charter of Fundamental Rights of the European Union or that it is manifestly abusive'.⁸⁸

This provision was criticised by a number of stakeholders, who claimed that the 'E-Evidence proposals turn service providers into judicial authorities'.⁸⁹ Indeed, as Professor Böse noted in a study for the EP LIBE Committee, an important theme is the concern about 're-allocation of protective functions'⁹⁰ from states to service providers. Taking into consideration the important powers of review conferred on service providers by the Commission's proposals and, conversely, the almost complete lack of powers of review conferred on states other than the issuing state, Professor Böse and other commentators⁹¹ have questioned what the EDPB called the capacity of service providers to 'ensure the protection of personal data as efficiently as public authorities are able and obliged to do'.⁹²

The Council's draft reacted to the recognition of such powers for service providers by removing most of them and weakening others. As a result, only a skeleton of the initial protective powers conferred on service providers by the Commission's proposal remained in the Council's draft.

Sippel's Report proposed a more appropriate role for service providers. The logic was that the responsibility for protecting human rights should not be shifted from states to service providers, but that the latter *may* be able to provide critical information relevant to the assessment of the necessity and proportionality of orders.

The EP's draft followed this approach. A service provider cannot oppose the execution on human rights grounds. This responsibility has been transferred, instead, to the executing state which 'shall refuse' the execution of an EPO where 'there are substantial grounds to believe that the execution of the European Production Order would be incompatible with Member State's obligations in accordance with Article 6 TEU and the Charter'.⁹³ This was also the solution given by the final text of the Regulation.⁹⁴

Another interesting issue is that the Commission's proposal also provided that the service provider may refuse the execution of an EPO if it considers that compliance with the EPO would be in conflict with the applicable laws of a third country.⁹⁵ These grounds for non-compliance disappeared from the Council's and the EP's drafts and, of course, from the adopted Regulation. Nevertheless, as we will see in Section 7.4, these drafts afforded the service provider the ability to initiate a review procedure based on this element.

⁸⁸ Ibid., Arts. 9(5b) and 14(4f).

⁸⁹ According to a position posted by EDRI, 'EU "E-Evidence" Proposals Turn Service Providers into Judicial Authorities', EDRI, 17 April 2018, <https://edri.org/our-work/eu-e-evidence-proposals-turn-service-providers-into-judicial-authorities/>.

⁹⁰ Martin Böse, *An Assessment of the Commission's Proposals on Electronic Evidence* (study requested by the LIBE Committee of the EU Parliament) (Brussels: European Union, September 2018), 41, [www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU\(2018\)604989_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf).

⁹¹ See Valsamis Mitsilegas, 'The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-Evidence' (2018) 25(3) *Maastricht Journal of European and Comparative Law* 263–265; Franssen, 'The E-Evidence Proposal'; Stanisław Tosza, 'The Public Role of Private Actors: Internet Service Providers in the E-Evidence Proposal', *European Law Blog*, 20 September 2022, <https://europeanlawblog.eu/2022/09/20/the-public-role-of-private-actors-internet-service-providers-in-the-e-evidence-proposal/>.

⁹² EDPB Opinion 23/2018, 7.

⁹³ EP's draft, Art. 10a(1)(c).

⁹⁴ Regulation (EU) 2023/1543, Art. 12(1)(c).

⁹⁵ Ibid., Arts. 15 and 16.

Finally, it is interesting to note that the Council's draft introduced a provision according to which 'Member States shall ensure that pecuniary sanctions of up to 2% of the total worldwide annual turnover of the service provider's preceding financial year can be imposed' in the event of non-compliance.⁹⁶ This could have a chilling effect on service providers that wish to challenge the legality of an EPO. The EP's draft abandoned this idea by providing instead that 'the sanctions provided for by national laws of the Member States shall be effective, proportionate and dissuasive'.⁹⁷ The adopted Regulation reintroduced, nonetheless, the Council's language.⁹⁸ It also introduced an important provision according to which 'service providers shall not be held liable in Member States for the consequences resulting from compliance' with an EPO.⁹⁹

7.3.7 *Conflict of Laws*

The problem of conflict of laws was another very important issue discussed during the E-Evidence negotiations. E-Evidence imitates the CLOUD Act in enabling EPOs to potentially have extraterritorial reach: the issuing authority of a member state may order a service provider 'offering services in the Union' to produce electronic evidence 'regardless of the location of data'.¹⁰⁰ To the extent that such EPOs might be addressed to US or other countries' companies, they might conflict with the laws and blocking statutes of these third states. Similarly, the fundamental interests of such third states, which include national security and defence, trade secrets and human rights considerations, might militate against the disclosure of certain types of data to the issuing member state.

With regard to the US, for example, as already mentioned, the Stored Communications Act (SCA), in Title II of the ECPA, is a blocking statute that prohibits US-based providers from turning over the content of communications to foreign governments.¹⁰¹ Application of E-Evidence might give rise to significant disputes with the US (or any other third state that has similar blocking statutes). E-Evidence would indeed require production of evidence, while the blocking statute would forbid it. To mitigate such risks, the Commission's proposal introduced an effective mechanism to resolve conflict of laws. However, the Council's draft significantly downgraded those protections.

Indeed, Articles 15 and 16 of the Commission's proposal provided for two different review procedures in case service providers issued with an EPO consider that compliance with the EPO would be in conflict with the applicable laws of a third country. Article 15 established a 'Review procedure' in the event of conflicting obligations based on the 'protection of fundamental rights of individuals' or 'fundamental interests of a third country related to national security or defense'. It provided that the addressee, if it considered that such a conflict of laws existed, should inform the issuing authority of the reasons why it did not execute the EPO. If the issuing authority intended to uphold the EPO, it should request that a review be undertaken by the competent court within that member state. If the competent court found that there was *no conflict* (either because the third country's law did not apply or because it did not prohibit disclosure of the data

⁹⁶ Ibid., Art.13(c).

⁹⁷ EP's draft, Art.13.(1)

⁹⁸ Regulation (EU) 2023/1543, Art. 15(1).

⁹⁹ Ibid., Art. 15(2).

¹⁰⁰ Ibid., Art. 1(1).

¹⁰¹ The CLOUD Act enabled foreign governments to conclude an 'executive agreement' with the USA. Such an executive agreement would lift the blocking statute for requests covered by the agreement. The elimination of the blocking statute, however, is limited to situations where an executive agreement is in force (and no such agreements are in force today), and may only concern the data of foreign citizens who reside outside of the US.

requested, or because it manifestly sought to protect other interests than those mentioned just now), then the order should be upheld. If, on the other hand, the court found that *there was* a conflict, it had an obligation to ‘transmit all relevant factual and legal information as regards the case, including its assessment, to the central authorities in the third country concerned’. The third country was then entitled to object to the order within a maximum of fifty days, at which point the court had an obligation to lift the order. Article 15 therefore provided for a review mechanism which allowed, assuming that the various conditions were met, affected third states to exercise their protective function in relation to human rights and/or to protect their own state interests by *preventing* the execution of an EPO.

Article 16 established a ‘Review procedure’ in the event of conflicting obligations based on ‘*other grounds*’ than those mentioned in Article 15. This procedure was very different: the competent court had *no obligation* in this case to notify the third state authorities of a potential conflict of laws. Furthermore, it had *no obligation to dismiss* the order if it concluded that such a conflict of laws existed. Article 16 therefore intended to give *discretion* to the Court in this respect, while setting out the factors that should be considered in determining whether to uphold or withdraw the order.

With regard to the capacity of Article 15 to prevent conflict of laws, it is important to note that the EDPB, which had hitherto been critical of the Commission’s proposal, welcomed this article as a positive development. It emphasised that it ‘deems (it) essential that the proposal provides for the consultation of third-countries [*sic*] authorities, at least where a conflict arises, as well as the obligation to lift the order when a third country’s authority raises an objection’.¹⁰²

The Council, however, set out changes that went in the opposite direction to those supported by the EDPB. Far from following the EDPB recommendations, the Council removed all the enhanced protections contained in the Commission’s proposal. In particular, it substantially reduced the influence that the authorities in the third country can have in the process. It also removed the obligation of the competent court of the issuing country to dismiss the order if it finds that there is a conflict of laws. The court of the issuing country instead, henceforward, had discretion to dismiss the order only after weighing a series of relevant factors. This was the solution adopted, with the blessing of the EP, in the final text of the Regulation.¹⁰³

7.4 A PROJECT LOST IN NOTIFICATION

Let’s now turn to what has been the *main* obstacle to the E-Evidence negotiation process over the past four and a half years. We will start by looking at how the Commission’s initial draft excluded any a priori notification, as it was founded on the idea of a kind of ‘absolute mutual trust’ among EU member states. We will then examine the changes proposed in the Council’s draft, Sippel’s Report and the EP’s final compromise draft. We will end with a few observations about the solutions given to these issues by the final text of the Regulation.

7.4.1 The Commission’s Initial Approach Based on Mutual Trust

The Commission’s draft was based on the idea that the draft Regulation ‘can only work on the basis of a high level of mutual trust between the Member States’.¹⁰⁴ The Commission’s logic was that there was no need for a review to be conducted because member states were expected to trust

¹⁰² EDPB Opinion 23/2018, 17–18.

¹⁰³ See Regulation (EU) 2023/1543, Art. 17.

¹⁰⁴ Commission’s draft, Rec. (11).

one another's legal and judicial systems. The actions of the authorities of the issuing member state were deemed to be sufficient and trustworthy.

As a result, the Commission's draft did not provide for any a priori notification mechanism in relation to another member state. It assigned only a limited reviewing role to the enforcing member state (i.e., the member state where the service provider is established). Two mechanisms appeared in this regard in the EC's proposal.

First, the proposal envisioned certain situations in which the issuing authority 'has to seek clarification before issuing the European Production Order, including by consulting the competent authorities of the Member State concerned'. This is especially the case when the issuing authority has reason to believe that (i) transactional or content data that has been requested is protected by immunities and privileges granted under the law of the member state where the service provider is established, or (ii) its disclosure may impact the fundamental interests of the enforcing member state such as national security and defence.¹⁰⁵

Second, the enforcing member state is given the option of refusing to enforce an EPO if it considers 'that the data concerned is protected by an immunity or privilege under its national law or its disclosure may impact its fundamental interests such as national security and defence'.¹⁰⁶ This mechanism is, however, applied only during the latter stages of the *enforcement* of an EPO, that is, when a service provider does not comply with an EPO and the issuing state therefore needs to request the intervention of the enforcing state. If the service provider complies with an EPO, which in turn affects the fundamental interests of another member state or the fundamental rights of its citizens, the affected member state may not even be made aware of this having occurred, let alone be able to object.

These proposals, which are based on 'a high level of mutual trust', arrived at a time when 'mutual trust' was being 'questioned with increased intensity'.¹⁰⁷ First, one should recall that there has been, over the last few years, mounting concern about the 'rule-of-law backsliding' in certain member states, such as Hungary and Poland. Second, EU member states' criminal law systems are so different that this could affect the trust they have in each other's systems in general. Third, even if 'a high level of mutual trust' existed today among EU member states, it would still not provide an absolute guarantee that the issuing state would protect the fundamental interests of other member states and the human rights of their residents. Indeed, there is a fear that the authorities of the issuing state will prioritise their own interests over foreign interests. If the judicial authorities of the issuing state consider that access to data stored in another member state is critical in terms of their ability to resolve an important criminal case, they might take strong measures to access this data, downsizing the interests of other member states, assuming, of course, that there are other member states involved. Therefore, it is easy to understand why several states considered the Commission's initial proposal to be unsatisfactory during the discussions at the Council.

7.4.2 *The Council's 'General Approach': A Toothless Notification to the Enforcing Member State*

During the debates at the Council some delegations advocated going one step further than the Commission's proposals, namely, introducing a notification mechanism that involves other

¹⁰⁵ Ibid., Art. 5(7).

¹⁰⁶ Ibid., Art. 14(2).

¹⁰⁷ Tosza, 'All Evidence Is Equal', 182 who also refers to Auke Willems, 'The Court of Justice of the European Union's Mutual Trust Journey in EU Criminal Law: From a Presumption to (Room for) Rebuttal' (2019) 20 *German Law Journal* 468–495.

member states than the issuing state. For these delegations, introducing a notification mechanism would be useful for a number of reasons. It would aid in finding a balance between fighting crime and protecting other values. It would also help address the fact that the authorities of the issuing state are not always in the best position to assess the EPO properly, as they may lack the necessary information about its potential impact. Notification could also improve the efficiency of the instrument, while safeguarding fundamental rights and introducing legal certainty. These states also considered that such a notification procedure would help transfer the burdensome tasks involved in assessing whether the orders are compatible with human rights and other fundamental values, from the providers to the authorities, thus avoiding the spectre of the ‘privatization of law enforcement’ mentioned in Section 7.3.6. They also claimed that it would help safeguard national security and the public interest, and not slow down the E-Evidence mechanism, as the strict deadlines involved in this project would be maintained.

Other member states opposed a notification system, a few of them strongly. Others again were more flexible, declaring that they would be open to a compromise that permits a balanced approach and enables the Regulation to be adopted quickly. All these states referenced a number of reasons for opposing the introduction of a notification procedure, arguing that such a mechanism would, among other things, undermine mutual trust between member states. They also claimed that notification would damage the basic operational structure and the very *raison d’être* of the proposal, by making the procedure even more burdensome than the EIO and by reintroducing the territoriality criterion via the back door. Such a notification system would also generate practical and technical difficulties (including the need to translate the orders into the language of the notified member states) and a very high workload for those member states that have many service providers or legal representatives within their territory.¹⁰⁸

The compromise that was found is based on an Austrian proposal and involves introducing a notification system of an informative nature. According to the Council’s draft, only the enforcing member state should be notified when the issuing authority requests *content* data and ‘has reasonable grounds to believe that the person whose data are sought is not residing on its own territory’.¹⁰⁹ Furthermore, the Council’s draft provides that notification ‘shall not have suspensive effect on the obligations’¹¹⁰ of the service provider to respond to an EPO. This means that even if the enforcing state eventually rejects the order, the service provider may already have given the data to the issuing state.

7.4.3 Sippel’s Draft Report: A Double Notification Mechanism

Sippel’s Report took an entirely different approach from the Council’s draft. The Report was founded not on ‘absolute’ mutual trust (per the Commission’s version) but on the idea that arguments about efficiency should not override the need to protect fundamental rights. It claimed, nonetheless, that efficiency would not be significantly affected to the extent that the time frame proposed by the Commission was safeguarded.

The most important change proposed by Sippel’s Report was the introduction of a double notification mechanism: it meant that both the ‘executing State’ (i.e., the state where the service

¹⁰⁸ As Commissioner Věra Jourová stated, ‘Ireland for instance would have to hire an army of new administrators only because Google and Facebook are based on their territory’. See Theodore Christakis, ‘Big Divergence of Opinions on E-Evidence in the EU Council: A Proposal in Order to Disentangle the Notification Knot’, *Cross Border Data Forum*, 22 October 2018, www.crossborderdataforum.org/big-divergence-of-opinions-on-e-evidence-in-the-eu-council-a-proposal-in-order-to-disentangle-the-notification-knot/.

¹⁰⁹ Council’s draft, Art. 7a(1).

¹¹⁰ Ibid., Art. 7a(4).

provider is established, which was called ‘enforcing State’ in the Commission’s draft) *and* the state of residence (the ‘affected State’) would be notified, where the latter is known to be different from the ‘issuing’ and the ‘executing’ state. In Sippel’s mind, such a double notification mechanism would permit EU member states to exercise their traditional protective function, but also to ensure that fundamental rights are respected on their territory. It is interesting to dive a little bit further into Sippel’s proposals to examine whether this complicated system of notifications permits striking the right balance between protection and efficiency.

Let’s examine first the introduction of the affected state (the member state of permanent residence of the affected person) being notified, which was undoubtedly the main novelty in Sippel’s Report. The author of this chapter has argued a number of times¹¹¹ in favour of notifying the ‘affected’ state (instead of the ‘executing’ state), considering that such a notification provides a higher degree of protection, while preserving efficiency. Notifying the affected state has the great advantage of bringing the targeted individual back into the equation. The member state of residence would be able to exercise its traditional protective function concerning the human rights of the targeted individual. It would have a much greater incentive to do so than the enforcing state (where the service provider is based) which, most of the time, has a weak link to a criminal case. Moreover, such a notification may permit the sovereign prerogatives and fundamental interests of the member state in which the data subjects reside to be protected, including the national security of the member state of residence (if, for instance, the targeted person is an official of the notified member state), trade secrets (if the target is a business executive) and other essential interests.

In response to Sippel’s Report, the Commission claimed¹¹² that the system would be too burdensome for LEAs. That is partly true, as Sippel’s Report recommended introducing such a notification requirement for all types of data, including subscriber and access data. If, however, notifying the affected state concerned only the most sensitive forms of data in terms of human rights, namely, content and transactional data, such a notification system would remain efficient.

Indeed, the time frame of ten days proposed by the Commission and the Council within which the affected state, where applicable, would be able to object to an EPO would remain entirely feasible. Efficiency is affected much less than is generally assumed, because in most cases (93 per cent according to one service provider¹¹³), the investigating/issuing authority seeks data on its own residents. Therefore, in contrast to MLAT requests, which require that other countries be notified in 100 per cent of cases, the ‘affected state’ provision would be applicable in only about 7 per cent of cases. Based on this data, and the calculations of the author of this chapter,¹¹⁴ it seems reasonable to believe that the twenty smallest EU member states would be notified as the ‘affected state’ no more than a few dozen times per year.

The burden should therefore be small and manageable for them. If one considers that in 2018 Facebook received and examined a total of 53,841 data requests, Google received 47,011, Apple 43,480 and Microsoft 22,919,¹¹⁵ it would be an insult to medium-sized EU countries like Sweden or Austria to

¹¹¹ For a detailed analysis, see Christakis, ‘Lost in Notification?’. See also Christakis, ‘Big Divergence’ and Theodore Christakis, ‘E-Evidence in the EU Parliament: Basic Features of Birgit’s Sippel’s Draft Report’, *European Law Blog*, 21 January 2020, <https://europeanlawblog.eu/2020/01/21/e-evidence-in-the-eu-parliament-basic-features-of-birgit-sippels-draft-Report/>.

¹¹² In the unpublished Commission’s Non-paper already mentioned.

¹¹³ Christakis, ‘Lost in Notification?’.

¹¹⁴ See *ibid.*

¹¹⁵ See Europol, *SIRIUS EU Digital Evidence Situation Report: Cross-Border Access to Electronic Evidence* (The Hague: Europol, 20 December 2019), 12, https://europol.europa.eu/cms/sites/default/files/documents/sirius_eu_digital_evidence_report.pdf.

argue that they would be incapable of examining a few dozen notifications per year in order to protect, as ‘affected’ states, the human rights of their populations and their sovereign interests.

The Commission’s argument in the non-paper that ‘notification to the affected State will go far beyond what exists under current mutual recognition and legal assistance instruments’¹¹⁶ also appears doubtful. Including the concept of the ‘affected state’ in the E-Evidence package, as Sippel suggested,¹¹⁷ would have permitted the adoption, in an appropriate way, of protections in the ‘digital world’ that were already available ‘in the physical world’ under MLA systems.¹¹⁸ In conclusion, the burden for affected states should be small and the ‘protecting human rights/sovereign interests benefit’ to them and their populations should be important. However, as we will see, the compromise reached at the EP abandoned the idea of notifying the affected state, and this idea never really re-emerged during the trilogues – despite the importance attributed by the Council, as we will see, to the place of residence of the data subject.

Sippel’s Report also provided for a requirement to systematically notify the executing state at the time of the issuance of an EPO. While notifying the affected state (if the state of residence of the person whose data is sought is other than the issuing state) made real sense for the reasons explained already, notifying the executing state seemed less compelling. Imagine that a crime has been committed in France. The victim is French, and the suspect is a French person and resident. What is the point of obliging France to notify Ireland simply because the service provider of the suspect is established in Ireland or has its legal representative there? Despite the fact that notifying the executing state is of less relevance, and its link to a criminal case is often very weak or inexistent, this idea is strongly imprinted in the minds of various stakeholders.

With regard to Sippel’s Report, there is no doubt that notifying the executing state, when combined with notifying the affected state, would have offered important additional protections and guarantees. In Sippel’s mind, the involvement of the executing state was absolutely necessary in order to resolve conflicts of law or rule-of-law problems. It was also necessary in order to provide a solid legal basis for E-Evidence, namely, Article 82 TFEU, based on the notion of cooperation between two judicial authorities.

The EP Rapporteur introduced the concept of the ‘executing’ state (as opposed to the ‘enforcing’ state in the Commission’s draft) which would automatically be involved in all EPOs thanks to this notification system and would have been considered as having automatically recognised the EPO Certificate (unless, of course, it raised grounds for refusal). Despite this strong protective logic behind Sippel’s proposal,¹¹⁹ the double notification system would have undoubtedly created a huge burden for the executing state and was considered particularly unattractive and problematic by LEAs.

7.4.4 *The EP’s Approach*

The EP tried to address the frustration of LEAs with Sippel’s Report by reaching a compromise which removed the need to notify the affected state but maintained a strong notification mechanism in relation to the ‘executing’ state. In the EP’s draft, four different regimes of notification in relation to the ‘executing’ state were proposed.

Firstly, the issuing state should simultaneously address an EPO for ‘subscriber data and IP addresses for the sole purpose of identifying a person’ to the service provider and the authority of

¹¹⁶ Unpublished Commission’s Non-paper already mentioned.

¹¹⁷ Sippel’s Report.

¹¹⁸ For explanations, see Christakis, ‘Lost in Notification?’.

¹¹⁹ Ibid.

the ‘executing’ state. In such a case, however, such a notification would not have a suspensive effect.¹²⁰

Secondly, if the request concerned ‘traffic or content data’, the same notification would be required and this time it would have a suspensive effect. If the executing state did not invoke one of the grounds for refusal specified below within ten days (or sixteen hours in cases where there was an emergency), the service provider to which the order was addressed should ensure that the requested data was immediately transmitted directly to the issuing authority.¹²¹

Thirdly, a specific mechanism was introduced for the first time if the issuing country was subject to Article 7 TEU procedures. The EP’s draft provided:

Where the issuing State is subject to a procedure referred to in Article 7(1) or 7(2) of the Treaty on European Union, the service provider shall transmit the requested data only after receiving the explicit written approval of the executing authority. For this, the executing authority shall assess the order of the issuing authority with due diligence and check in particular for grounds for non-recognition or non-execution pursuant to Article 10a before giving its written approval within the deadlines [presented above].¹²²

Fourthly, the EP’s draft also provided for the executing state to be notified about preservation orders, but this would not have a suspensive effect.¹²³

For all the categories mentioned here, the EP’s draft recognised a long list of grounds for refusal in favour of the notified executing state. The latter was obliged to refuse the order when four scenarios occurred, including when ‘there [were] substantial grounds to believe that the execution of the EPO would be incompatible with the Member State’s obligations in accordance with Article 6 TEU and the Charter’, or when ‘there is an immunity, a privilege or rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media under the law of the executing State, which makes it impossible to execute the EPO’.¹²⁴ The notified executing state also had the power (but not an obligation) to reject the order in four other scenarios, including when the execution of the EPO ‘would harm essential national security interests, jeopardise the source of the information or involve the use of classified information relating to specific intelligence activities’.¹²⁵

7.4.5 The Solutions Finally Given by the Regulation

Despite the fact that the EP’s draft proposed a notification mechanism that was ‘softer’ than the one proposed in Sippel’s Report, the EP’s proposal was still a red flag for the Council and the EU member states, whose LEAs considered that these proposals would render the whole E-Evidence Regulation burdensome and inefficient. The two European co-legislators agreed fairly quickly that a compromise pack should not include notification for (1) preservation orders or (2) EPOs in relation to subscriber data and ‘traffic data for the sole purpose of identifying a person’. In exchange for this, the Council agreed that the notified authority should be afforded the right to refuse EPOs, based on a list of grounds for refusal.

The two co-legislators disagreed, nonetheless, on a very important issue. The Council insisted that there should be no notification when ‘there are no grounds to believe that the person whose

¹²⁰ EP’s draft, Art. 8a(1).

¹²¹ Ibid., Art. 9(2b).

¹²² Ibid., Art. 9(2a).

¹²³ Ibid., Art. 10(1a).

¹²⁴ Ibid., Art. 10a(1).

¹²⁵ Ibid., Art. 10a(2).

data are sought is not residing on the territory of the issuing State’.¹²⁶ The Parliament, however, continued to insist on a mandatory notification system ‘for all orders concerning traffic or content data, irrespective of the basis for the criminal proceedings in the issuing Member State for which those data are required’.¹²⁷

The Council finally won on this point. Regulation (EU) 2023/1543 provides in Article 8(2) that the notification requirement

shall not apply if, at the time of issuing the order, the issuing authority has reasonable grounds to believe that:

- (a) the offence has been committed, is being committed or is likely to be committed in the issuing State; and
- (b) the person whose data are requested resides in the issuing State.

7.5 CONCLUSION

The present chapter has tried to illustrate all the challenges that the ambitious E-Evidence legislative package has faced. E-Evidence represents a major paradigm shift in police and judicial cooperation with service providers in the EU: for the first time, national investigating authorities will be able to make a direct request to service providers in other member states to hand over or secure electronic evidence, through production or preservation orders, backed by clear deadlines and uniform rules across the EU. For the first time, service providers will be compelled by European law to comply with such orders, irrespective of their country of establishment or the location of the data. The expectation is that this legislative package, which is based on direct cooperation between the authorities of one EU country and the service provider(s) of another, will greatly improve the efficiency of cross-border criminal investigations and resolve a great deal of practical and legal problems that LEAs around Europe are facing today in more than half of all criminal investigations.

This ambitious new direct cooperation mechanism also raises, nonetheless, a lot of new legal issues and poses a number of risks related to fundamental rights, in particular privacy and data protection, but also procedural rights, due to important differences in criminal law across the EU. The difficult negotiations that have characterised the E-Evidence project are a reflection of the struggle that EU institutions have experienced to find a satisfactory compromise on a number of tricky issues, ranging from human rights to conflicts of laws issues, and from what constitutes an appropriate role for service providers to the major Gordian knot of notification between member states. Unlike the solution given by Alexander the Great for untying the impossibly tangled Gordian knot (he drew his sword and sliced it in half with a single stroke), there has been no easy solution to the notification problem in E-Evidence.

The author of this chapter proposed¹²⁸ that the solution to this problem could be to solely notify the ‘affected state’ and combine this with a specific mechanism (such as the one eventually proposed by the Parliament) that enables orders issued by countries subject to Article 7 TEU procedures to be dealt with. As explained earlier, this approach had the great benefit of effectively protecting human rights (thanks to the involvement of the state that has

¹²⁶ See Le comité des représentants permanents, Lettre du Conseil à Mme Sippel.

¹²⁷ See Presidency of the Council, Regulation on European Production and Preservation Orders for electronic evidence Directive on legal representatives for gathering evidence – Progress report, 9296/22, 23 May 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9296_2022_INIT&from=EN, emphasis added.

¹²⁸ See Christakis, ‘Big Divergence’ and Christakis, ‘Lost in Notification?’.

territorial jurisdiction over its residents, as well as an incentive and an obligation to protect them), without hindering the efficiency of the new direct cooperation mechanism.

However, this approach was opposed by several states as well as MEPs for two main reasons: the first one was that it would be hard for the authorities of the issuing state to identify the country of residence of the data subject; the second came from those who insisted that, even if the data in question is overwhelmingly held by US service providers that have a legal representative in the EU, requests might also concern EU providers, such as EU telecom operators or European cloud providers, created and established in specific EU member states. The argument then was that notification to the enforcing state (where the service provider is established) was the only way to make sure that the member states of these EU providers will be informed about requests addressed to their national champions by foreign states. So, taking into consideration that notifying simultaneously two different kinds of state (both the enforcing and the affected one) was an unacceptable option for EU LEAs, the only way was to ‘eliminate’ from the equation of notification the affected state.

Interestingly, while both the Council and the Parliament rejected the proposal to notify the affected state, they espoused one of the building blocks underlying this proposal: as we have seen, the criterion of residence of the targeted data subject does play a major role in the final Regulation, as notification of the state where the service provider is established will take place only if there are reasons to believe that the person whose data is sought does not reside on the territory of the issuing state.

Curiously, though, while the legislators acknowledged the fundamental importance of the place of residence of the data subject, they seem to have drawn the wrong conclusion about which country should be notified: instead of notifying the state in which the data subject resides, the country in which the service provider is located will be notified. If, for instance, Bulgaria wishes to access the data of a German person which Bulgaria knows resides in Berlin, Germany will not be notified, but Bulgaria will need to notify Ireland, where the service provider (Google, for instance) has its legal representative.

Arguably, the advantage of this mechanism is its simplicity: only two states are involved (the issuing and the executing states), while notifying the affected state requires the involvement of three types of state: the issuing state; the affected state, when the targeted data subject resides in a country other than the issuing state; and the executing state, when a service provider refuses to execute the order and/or when the issuing state is subject to Article 7 TEU procedures – a situation that a notification system that solely notifies the affected state cannot address as such. It remains to be seen, however, whether the executing states (especially Ireland and Luxembourg, where the main US service providers are established) will effectively play the ‘responsibility to protect’ role that E-Evidence wishes to entrust to them.

In any case, it is a positive development that the final draft of E-Evidence will be more protective of human rights than the initial draft introduced by the Commission, while still preserving the required efficiency with regard to criminal investigations desired by the Commission. The co-legislators have also agreed on a framework for an EU-wide platform through which orders to service providers, but also data to authorities, will be transmitted. Such an EU platform is the best way for service providers to be sure that an order is genuine and has not been falsified, and to guarantee that confidential data is safely and securely shared with investigating authorities.

Under the Regulation, service providers will be able to flag potential problems not only to the issuing authority but also to the authorities of the country in which they are located, for example if they think that orders might restrict media freedom. This seems to be a more appropriate role

for service providers than the initial ‘grounds for refusal’ role envisioned for them in the Commission’s draft. To the extent that only the issuing (or executing) state can decide whether there is a problem that requires the order to be modified or lifted, there should be no ‘privatization of law enforcement’. Service providers will still, nonetheless, be able to protect their clients by flagging issues that, eventually, neither the issuing authority nor the executing state will be able to see.

Last, but not least, the adoption of E-Evidence enabled the resumption of EU–US negotiations on a transatlantic agreement regarding access to data by LEAs. The conclusion of such an agreement could be very helpful in facilitating access to data by LEAs during criminal investigations, resolving important conflict of laws issues, introducing adequate human rights protections and creating legal certainty for services providers on both sides of the Atlantic.

Moving in the Right Direction for Transborder Access to Digital Evidence in Criminal Matters?

The Council of Europe and the Second Additional Protocol Introducing Direct Cooperation Mechanisms

Ma. Angela Leonor Aguinaldo and Paul de Hert

8.1 INTRODUCTION

More and more online *and* ordinary crimes are facilitated through the usage of computing devices that allow traces associated with crime to be left and are useful for law enforcement authorities.¹ Access to electronic data for evidence purposes has become indispensable to law enforcement authorities as people are currently living in a digital and digitized world.²

There is also the growing importance of accessing this electronic evidence internationally.³ Law enforcement authorities reactively attempt to go global with or without the necessary legal frameworks. In particular they want and seek direct cooperation with service providers.⁴ The lack of a legal framework surrounding this globalized law enforcement inevitably leads to a clash between different players and to questions concerning international law, sovereignty,

¹ B. Blažič and T. Klobučar, *Advancement in Cybercrime Investigation: The New European Legal Instruments for Collecting Cross-Border E-evidence* (Cham: Springer, 2019), 858; E. De Busser, “The Digital Unfitness of Mutual Legal Assistance” (2017) 28 *Security and Human Rights* 161, 171; J. de Souza Abreu, “Jurisdictional Battles for Digital Evidence, MLAT Reform, and the Brazilian Experience” (2018) 55 *Revista de Informação Legislativa* 233, 234; I. Walden, “Crime and Security in Cyberspace” (2005) 18 *Cambridge Review of International Affairs* 51, 51.

² The Council of the European Union (EU) has acknowledged its usefulness in law enforcement investigations in its *Conclusions on Retention of Data for the Purpose of Fighting Crime*, No. 10083/19, May 27, 2019, 5, <https://data.consilium.europa.eu/doc/document/ST-9663-2019-INIT/en/pdf>. See also M. A. Biasiotti, “Present and Future Exchange of Electronic Evidence in Europe,” in M. A. Biasiotti, J. P. M. Bonnici, J. Cannataci and F. Turchi (eds.), *Handling and Exchanging Electronic Evidence Across Europe* (Cham: Springer, 2018), 14; J. Bonnici, M. Tudorica and J. Cannataci, “The European Legal Framework on Electronic Evidence: Complex and in Need of Reform,” in M. A. Biasiotti, J. P. M. Bonnici, J. Cannataci and F. Turchi (eds.), *Handling and Exchanging Electronic Evidence Across Europe* (Cham: Springer, 2018), 190; E. De Busser, “EU-US Digital Data Exchange to Combat Financial Crime: Fast Is the New Slow” (2018) 19 *German Law Journal* 1251, 1252; B. Hayes, J. Jeandesboz, F. Ragazzi, S. Simon and V. Mitsilegas, “The Law Enforcement Challenges of Cybercrime: Are We Playing Catch Up?,” Think Tank, European Parliament, October 28, 2020, 20, [www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU\(2015\)536471](http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)536471); A. Seger, “E-Evidence and Access to Data in the Cloud Results of the Cloud Evidence Group of the Cybercrime Convention Committee,” in M. A. Biasiotti, J. P. M. Bonnici, J. Cannataci and F. Turchi (eds.), *Handling and Exchanging Electronic Evidence Across Europe* (Cham: Springer, 2018), 40.

³ Biasiotti, “Present and Future Exchange,” 14.

⁴ For how law enforcement authorities around the world look for alternatives that are less time-consuming and more straightforward in crimes that are international and involving digital evidence, see De Busser, “The Digital Unfitness,” 168; P. De Hert, C. Parlar and J. Thumfart, “Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders: From Yahoo Belgium to Microsoft Ireland” (2018) 9 *New Journal of European Criminal Law* 326, 328.

jurisdiction, territorial prosecution, privacy rights and data security.⁵ Apart from legal problems, informal globalized law enforcement also encounters difficulties of obtaining electronic evidence because of its inherent volatility and transnational nature.⁶

The legal system needs to find solutions to address these legal and practical concerns.⁷ International or transnational cooperation in the exchange and transfer of evidence is made presently possible through mutual legal assistance in criminal matters (MLA).⁸ In terms of digital evidence, MLA is presented as an imperative and classic international cooperation instrument to facilitate its cross-border transfer as well as any access and exchange.⁹ However, these assistance procedures, when used for obtaining or accessing extraterritorial data, are believed to be neither efficient nor sufficient.¹⁰ In response, many states try to make the MLA system obsolete by resorting either (1) to *data localization* or *nationalization*, which compels service providers and tech companies to localize and keep data within the confines of their territorial jurisdiction; or (2) to *jurisdictional expansion*, which overstretches a state's jurisdiction over data regardless of where data is located.¹¹

⁵ Biasiotti, "Present and Future Exchange," 14; De Busser, "The Digital Unfitness," 163; Hayes et al., "The Law Enforcement Challenges," 43. See also J. F. Hill, "Problematic Alternatives: MLAT Reform for the Digital Age" (2015) *Harvard Law School National Security Journal*, <https://harvardnsj.org/2015/01/28/problematic-alternatives-mlat-reform-for-the-digital-age/>; A. Berkes, "Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control" (2019) 52(3) *Israel Law Review* 197–231; F. Delerue, "Reinterpretation or Contestation of International Law in Cyberspace?" (2019) 52(3) *Israel Law Review* 295–326.

⁶ See Blažič and Klobučar, "Advancement in Cybercrime Investigation," 858. For difficulties specific to cloud computing and law enforcement, see I. Walden, "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent," in S. Pearson and G. Yee (eds.), *Privacy and Security for Cloud Computing* (Cham: Springer, 2013), 47; "CPDP 2019: Avoiding a Race to the Bottom in Cross-Border Access to Data," YouTube, February 12, 2019, www.youtube.com/watch?v=gfi8p78mpT8; A. Osula, "Transborder Access and Territorial Sovereignty" (2015) 31 *Computer Law & Security Review* 719, 720; A. Perloff-Giles, "Transnational Cyber Offenses: Overcoming Jurisdictional Challenges" (2018) 43 *Yale Journal of International Law* 191, 191; Seger, "E-Evidence and Access," 36; Walden, "Accessing Data in the Cloud," 47.

⁷ Biasiotti, "Present and Future Exchange," 14; B.-J. Koops and M. Goodwin, "Cyberspace, the Cloud, and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law" (2015) Tilburg Law School Research Paper No. 5/2016, 10; D. Silva Ramalho, "The Use of Malware as a Means of Obtaining Evidence in Portuguese Criminal Proceedings" (2014) 11 *Digital Evidence and Electronic Signature Law Review* 55, 56; J. Turner, "Managing Digital Discovery in Criminal Cases" (2019) 109 *Journal of Criminal Law and Criminology* 237, 249.

⁸ See, e.g., De Busser, "EU-US Digital Data Exchange," 1255; De Busser, "The Digital Unfitness," 163; De Hert, Parlar and Thumfart, "Legal Arguments," 327; Koops and Goodwin, "Cyberspace, the Cloud," 7; Perloff-Giles, "Transnational Cyber Offenses," 206; U. Sieber and C. Neubert, "Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty" (2017) 20 *Max Planck Yearbook of United Nations Law Online* 239, 245.

⁹ On the benefits for states to cooperate (upholding laws when and where they lack power, regulatory restraint, moderating effect on regulatory claims), see U. Kohl, *Jurisdiction and the Internet: Regulatory Competence Over Online Activity* (Cambridge: Cambridge University Press, 2007), 211–213.

¹⁰ G. Boulet and N. Hernanz, "Cross-Border Law Enforcement Access to Data on the Internet and Rule of Law Challenges in the EU" (2013) D6.6 *SAPIENT Policy Brief* 12; De Busser, "The Digital Unfitness," 163; De Hert, Parlar and Thumfart, "Legal Arguments," 327; de Souza Abreu, "Jurisdictional Battles," 246; Koops and Goodwin, "Cyberspace, the Cloud," 7; Osula, "Transborder Access," 20; Perloff-Giles, "Transnational Cyber Offenses," 206; Sieber and Neubert, "Transnational Criminal Investigations," 246. Some even say that the current MLA framework as regards digital evidence and/or information is highly dysfunctional and cannot keep up with globalized data: the framework does not account for data jurisdiction, fundamental notions of privacy vs. law enforcement, distinctions of data and so on, which consequently results in delays and other problems in executing requests and causes sovereignty and civil rights disputes. De Busser, "The Digital Unfitness," 162; de Souza Abreu, "Jurisdictional Battles," 241; Hayes et al., "The Law Enforcement Challenges," 44; Hill, "Problematic Alternatives"; Perloff-Giles, "Transnational Cyber Offenses," 201; L. Tosoni, "Rethinking Privacy in the Council of Europe's Convention on Cybercrime" (2018) *Computer Law & Security Review* 1198.

¹¹ C. Burchard, "Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 1" (2018) 7 *Zeitschrift für die internationale*

Reactions to those developments occur on the international or national level. For purposes of this chapter, however, the focus is on the legal responses to the law enforcement challenges formulated by the Council of Europe and the issues surrounding these responses.

In this chapter, we first discuss briefly the Council of Europe as a regional organization in the forefront of policymaking and/or laundering as regards digital evidence. Its story starts with the 2001 Cybercrime Convention (CC), the leading and most complete instrument tackling cybercrime (Section 8.2). We discuss the Convention provisions on international cooperation in criminal matters. Contracting parties (including not only European but also non-European states) shall afford each other the widest possible form of assistance in criminal matters. Mutual legal assistance (as opposed to unilateral state action) is provided by the Convention as the default route for cross-border exchange and transborder access to digital evidence. No explicit powers on (unilateral) transborder access were proposed in the 2001 text (due to a lack of agreement among the parties) except for the possibility of transborder access to publicly available data and transborder access to data based on consent (Art. 32 CC), which we will analyse in Section 8.3.

The most important reactions at the level of the Council of Europe were first interpretative Guiding Notes to the CC and most recently the adoption of the Second Protocol to the Convention. We briefly address the Guiding Notes (Section 8.4), but the main attention is paid to the Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence, which was opened for signature in May 2022 (Section 8.5). After presenting the main features of the Protocol (Sections 8.6–8.11), we provide some critical observations (Section 8.12) and overall conclusions (Section 8.13).

8.2 THE 2001 CYBERCRIME CONVENTION AND ITS CYBERCRIME CONVENTION COMMITTEE (T-CY)

Central in this contribution is the Council of Europe (CoE), a regional organization in its traditional sense of intergovernmentalism covering the whole of Europe (now forty-seven member states).¹² Not having a constitutional and fundamental framework, unlike its counterpart, the European Union (EU),¹³ the Council of Europe has no overarching authority that dictates policies and decisions to its member states and no heavyweight compliance mechanism that holds member states liable in case of non-compliance. Mainly informal and flexible, it has become a popular forum for international agreements equally among European states and non-European states.¹⁴ The organization contributes to harmonization of law through treaty-making, through

Strafrechtsdogmatik 52; P. De Hert and M. Kopcheva, “International Mutual Legal Assistance in Criminal Law Made Redundant: A Comment on the Belgian Yahoo! Case” (2011) 27 *Computer Law & Security Review* 291, 291; De Hert, Parlar and Thumfart, “Legal Arguments,” 326; Hill, “Problematic Alternatives.” For illustration on unilateralism, one can look into the US Cloud Act, the amendments made in the codes of criminal procedure of Germany and Belgium, as well as the Yahoo! Belgium case: D. Callaway and L. Determann, “The New US Cloud Act – History, Rules, and Effects” (2018) 35 *Computer & Internet Lawyer* 4.

¹² K. Rodriguez, D. O’Brien and M. Fernandez, “Behind the Octopus: The Hidden Race to Dismantle Global Law Enforcement Privacy Protections,” Electronic Frontier Foundation, August 1, 2018, 2, www.eff.org/deeplinks/2018/08/behind-octopus-hidden-race-dismantle-global-law-enforcement-privacy-protections. The Council of Europe was inspired by the idea of Winston Churchill of having a “United States of Europe” after the Second World War.

¹³ M. Hailbronner, “Beyond Legitimacy: Europe’s Crisis of Constitutional Democracy,” in M. Graber, S. Levinson and M. Tushnet (eds.), *Constitutional Democracy in Crisis?* (New York: Oxford University Press, 2018), 207.

¹⁴ F. Benoît-Rohmer and H. Klebes, *Council of Europe Law: Towards a Pan-European Legal Area* (Strasbourg: Council of Europe, 2005), 13; Rodriguez, O’Brien and Fernandez, “Behind the Octopus,” 2.

discussions of national laws at their respective drafting stages and through recommendations from its Council of Ministers to governments.¹⁵

Policymaking on criminal cooperation was comparatively slow in the EU in its early years. It was therefore the Council of Europe in the 1950s that took the lead with multilateral agreements at the international level on cross-border cooperation.¹⁶ Because of the increase in cybercrimes and the inadequacy of national laws addressing them, the CoE's Committee of Ministers adopted recommendation R89(9) *on computer-related crime* in 1989, which not only required member states to consider computer crimes in the review of their respective laws but also advocated the improvement of international cooperation.¹⁷ The same Committee in 1995 adopted recommendation R95(13) *on the harmonization of criminal procedural laws relating to information technology*, with procedures to better apply recommendation R89(9).¹⁸

In 1997, the CoE formed a Committee of Experts on Crime in Cyberspace, with the US government significantly participating in this effort.¹⁹ The product of these efforts, the CC (otherwise referred to as the Budapest Convention), was finalized on November 8, 2001 and opened for signature on November 23, 2001.²⁰ The Convention, together with a first protocol, harmonizes substantive law and aligns procedural laws applicable to criminal investigations with a digital component. It also sets up a system of international law enforcement and anti-cybercrime cooperation.²¹

The CC is the first and most significant multilateral binding instrument to regulate cybercrime and the most complete international standard to date.²² It addresses jurisdictional issues and harmonizes national substantive and procedural criminal law as well as

¹⁵ Benoît-Rohmer and Klebes, "Council of Europe Law," 13. For further elaboration on the "two Europes" and their respective similarities and differences, as well as an explanation of why and how the Council of Europe is the more favored international/regional forum nowadays as regards policymaking, see P. De Hert and A. Aguinaldo, "A Leading Role for the EU in Drafting Criminal Law Powers? Use of the Council of Europe for Policy Laundering" (2019) 10(2) *New Journal of European Criminal Law* 99–106.

¹⁶ The 1957 European Convention on Extradition and the 1959 European Convention on Mutual Legal Assistance in Criminal Matters, for instance, became core agreements in Europe; see S. Peers, "Mutual Recognition and Criminal Law in the European Union: Has the Council Got It Wrong?" (2004) 41 *Common Market Law Review* 5, 6.

¹⁷ S. Hopkins, "Cybercrime Convention: A Positive Beginning to a Long Road Ahead" (2003) 2 *Journal of High Technology Law* 101, 106; A. Osula, "Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study" (2016) 24 *International Journal of Law and Information Technology* 343, 348; A. Weber, "The Council of Europe's Convention on Cybercrime" (2003) *Berkeley Technology Law Journal* 425, 428.

¹⁸ Hopkins, "Cybercrime Convention," 106; Weber, "Europe's Convention on Cybercrime," 429. Despite these innovative recommendations, investigations at the national level continued to be slow and difficult to coordinate and many countries lacked the necessary cyber law statutes (Hopkins, "Cybercrime Convention," 106).

¹⁹ Hopkins, "Cybercrime Convention," 106; Weber, "Europe's Convention on Cybercrime," 429.

²⁰ Council of Europe, Convention on Cybercrime, ETS No. 185, November 23, 2001; Hopkins, "Cybercrime Convention," 106; Weber, "Europe's Convention on Cybercrime," 429.

²¹ R. Broadhurst, "Developments in the Global Law Enforcement of Cyber-Crime" (2006) 29 *Policing: An International Journal of Police Strategies & Management* 408, 410; Tosoni, "Rethinking Privacy," 2. There are presently fifty-six contracting states; accession to the agreement was not restricted to European member states but was likewise open to non-member states such as Canada, Japan, South Africa and the United States of America, among others. See Hopkins, "Cybercrime Convention," 106. The First Additional Protocol to the Cybercrime Convention entered into force on March 1, 2006 and presently has been ratified by thirty-two states. Council of Europe Treaties Office, "Details of Treaty No. 189," www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189. See also Broadhurst, "Developments in the Global Law Enforcement," 10. This Protocol tackles the criminalization of acts of a racist or xenophobic nature committed through computer systems as well as the inclusion of hate speech and child pornography to "content" cybercrime.

²² P. de Hert, C. Parlar and J. Sajfert, "The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist Transborder Access to Electronic Evidence Promoted via Soft Law" (2018) 34 *Computer Law & Security Review* 328; Hopkins, "Cybercrime Convention," 111; Walden, "Accessing Data in the Cloud," 47.

international cooperation in the field of computer crime and digital evidence.²³ One innovative feature is a framework for production orders allowing law enforcement authorities to obtain data from persons and providers within their territory (Art. 18 CC). Another feature is extended network search powers, that is, extending an existing search and seizure procedure of a computer system, or part thereof, and computer data stored therein in a house, building, dwelling or any other location in one's territory to data lawfully accessible by or available to the subject computer system (or part thereof) still within the same territory (Art. 19 CC).²⁴ This extended search should, however, remain within the national borders.²⁵ Transnational criminal investigations are dealt with by other provisions in the Convention, but these do not foresee extraterritorial powers that extend the domestic powers established in Articles 18 or 19 CC.

With the Convention came the establishment of the Cybercrime Convention Committee (otherwise referred to as the T-CY). This Committee represents the state parties to the Convention and must facilitate the effective use and implementation of the Convention, the exchange of information and consideration of any future amendments (Art. 46 CC).

8.3 THE 2001 CYBERCRIME CONVENTION AND ITS SILENCE ON TRANSBORDER ENFORCEMENT POWERS

There are no explicit unilateral transborder powers in the CC. As said, the Convention privileges assistance and cooperation, but there are some exceptions. It is closer to the truth to say that there is a “yes . . . but” situation on hand in the Convention system. Mutual legal assistance is the starting point, at least to believe the text of the Convention. It shall be provided to the “widest extent possible for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense” (Art. 25, §1 CC). Parties therefore must adopt legislative and other measures necessary to carry out obligations vis-à-vis MLA (Art. 25, §2 CC).²⁶

In our introduction (Section 8.1) we observed that legal practitioners on the law enforcement side have difficulties with this starting point. They often perceive MLA as “notoriously complex, slow and bureaucratic, particularly unsuitable for cloud-based” or even cyberspace-related investigations.²⁷ Often voiced in law enforcement circles, this view has had arguably a lasting impact on the drafting of the Convention, especially if one considers Article 32 in which two exempting circumstances are incorporated when international cooperation procedures are not required even though there is a transnational element: publicly available data and data available

²³ Broadhurst, “Developments in the Global Law Enforcement,” 10; Hayes et al., “The Law Enforcement Challenges,” 27; Sieber and Neubert, “Transnational Criminal Investigations,” 265; Walden, “Accessing Data in the Cloud,” 49; Weber, “Europe’s Convention on Cybercrime,” 425.

²⁴ Hayes et al., “The Law Enforcement Challenges,” 27; Walden, “Accessing Data in the Cloud,” 51.

²⁵ Koops and Goodwin, “Cyberspace, the Cloud,” 53; J. Pradillo, “Fighting Against Cybercrime in Europe: The Admissibility of Remote Searches in Spain” (2011) 19 *European Journal of Crime, Criminal Law and Criminal Justice* 363, 375; Walden, “Accessing Data in the Cloud,” 52. Stating it otherwise, the extended search would be sanctioned only on computers and servers within the state’s territory (Koops and Goodwin, “Cyberspace, the Cloud,” 53; Pradillo, “Fighting Against Cybercrime,” 375).

²⁶ Mutual legal assistance can be subject to the conditions provided under these respective domestic laws of the contracting states, including grounds to refuse assistance, except as may be otherwise provided for in the relevant provisions of the Convention (Art. 25, §5). One such relevant provision is Art. 27 CC, which states that absent any agreement or treaty in place between the parties allowing for MLA, its provisions shall apply.

²⁷ Walden, “Accessing Data in the Cloud,” 55. See also de Hert, Parlar and Thumfart, “Legal Arguments,” 328.

via consent.²⁸ The presence of these exempting circumstances does not seem to allow for other broader unilateral extraterritorial searches. As the drafters explained in the *Explanatory Report to the Convention in Cybercrime*, “it was not yet possible to prepare a comprehensive, legally binding regime regulating the area.”²⁹ But the Convention was not supposed to prejudice possible future developments toward unilateralism. The *Explanatory Report* contains a message in this regard, using Article 39, §3 with its cryptic terms,³⁰ as a basis.

Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof. In this regard, Article 39, §3 provides that other situations are neither authorised, nor precluded.³¹

As seen above, Article 39 is used as a legal basis to maintain a safe position that unilateral state actions other than what Article 32 provides are neither authorized nor precluded. Nevertheless, the coy and debatable, if not ambiguous, stance ultimately leaves member states ample discretion in their choice of action and avoids the necessary discussion about issues of human rights, privacy and sovereignty. A more acceptable interpretation would be that the CC does *not* allow transnational evidence gathering other than the two cases identified in Article 32 CC.³² *Expressio unius est exclusio alterius*.³³

8.4 THE PROCESS TOWARD UNILATERAL TRANSBORDER ACCESS THROUGH GUIDANCE NOTES

Accounts later came to light that transborder access has been occurring without a formal interstate process such as MLA. Law enforcement agents in many countries routinely turn to foreign service providers (often based in the US) to request and are provided with data from these providers, with the latter having readily available mechanisms to grant these

²⁸ First, with respect to publicly available data, authorization of another party is not required, regardless of where this data is located geographically (subparagraph a). In a second scenario a party accesses non-publicly available data through a computer system in its territory if the party “obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the party through that computer system” (subparagraph b). See Sieber and Neubert, “Transnational Criminal Investigations,” 266, 274; Weber, “Europe’s Convention on Cybercrime,” 433.

²⁹ This failure to have an agreement on remote extraterritorial searches was attributed to the Committee’s lack of experience with such situations and the “notions that the permissibility of unilateral assertions of power would turn on the precise circumstances of the individual case, thereby making it difficult to formulate general rules.” Council of Europe, *Explanatory Report to the Convention on Cybercrime*, ETS No. 185, November 23, 2001, para. 293.

³⁰ Article 39, §3 CC states: “Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.”

³¹ *Explanatory Report to the Convention on Cybercrime*, para. 293.

³² This view was reinforced by the Guidelines of the Council of Europe, which state that law enforcement authorities “should be encouraged not to direct requests directly to non-domestic internet service providers,” but should make use of interstate procedures contained in international cooperation treaties. Council of Europe, *Guidelines for the Cooperation between Law Enforcement and Internet Service Providers Against Cybercrime*, April 1–2, 2008, Guideline 36; D. Bigo, G. Boulet, C. Bowden, S. Carrera, J. Jeandesboz and A. Scherrer, *Fighting Cybercrime and Protecting Privacy in the Cloud* (Brussels: European Parliament, 2012), 32, www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET%282012%29462509_EN.pdf; Koops and Goodwin, “Cyberspace, the Cloud,” 58; Walden, “Accessing Data in the Cloud,” 59; I. Walden, “Law Enforcement Access to Data in Clouds,” in C. Millard (ed.), *Cloud Computing Law* (Oxford: Oxford University Press, 2013), 301.

³³ This Latin sentence literally means “the expression of one thing is the exclusion of the other.” This is a common law principle for construing legislation which holds that a syntactical presumption may be made that an express reference to one matter excludes other matters.

requests.³⁴ This is expected to some degree because digital evidence is normally in the custody of these private sources.³⁵

The foregoing served as part of the backdrop for the 6th Plenary Session of the Cybercrime Convention Committee (November 23–24, 2011) to discuss possible ways to enable and regulate in the Convention the issue of transborder access to data via an amendment, protocol or recommendation. For this task, the Committee created an ad hoc subgroup on jurisdiction and transborder access to data and data flows, composed of law enforcement experts.³⁶ In December 2012, the Committee adopted the report of this expert group and gave it an additional mandate to prepare a first draft text of a possible protocol to the Convention.³⁷

Amending a treaty and attending the necessary ratifications takes time, however, while agreeing on soft law instruments would require less time and could still do the job.³⁸ Therefore the T-CY changed its strategy and issued Guidance Notes in the meantime. Significant to our discussion are Guidance Notes Nos. 3 and 10,³⁹ on transborder access (Art. 32 CC) and domestic production orders for subscriber data and other forms of computer data (Art. 18 CC), respectively. These Guidance Notes are game-changers. As indicated in their preambles, they supposedly embody the “mutual understanding of the parties.”

We expound on these Guidance Notes and how they have shaped policy in a different contribution.⁴⁰ For the purposes of this chapter, though, what matters is that these Guidance Notes arguably have a creeping effect that provide broader interpretations expanding the applicability of the CC’s provisions on unilateral enforcement and transborder access to digital evidence.

On the one hand, Guidance Note No. 3 on transborder access (Art. 32 CC) confirms that unilateral transborder access without the need of MLA is applicable only in two scenarios provided by Article 32 CC, namely publicly available data and data that is available not publicly but with consent. There is no issue with the former but, allegedly, certain confusions exist with the latter due to divergencies in domestic practices and concerns over defense rights, privacy and sovereignty. Thus, Guidance Note No. 3 supposedly helps to “correct misunderstandings regarding transborder access” and to “reassure third parties” by addressing at least six points: (1) flexibility in extended searches in an international context; (2) non-imposition of *a posteriori* notifications albeit this is generally indispensable on data protection considerations; (3) definition of what constitutes consent; (4) who may give it; (5) when it should be given; and (6) where it should be given. In providing these six “clarifications,” the Guidance Note effectively expands

³⁴ See in more detail A. Aguinaldo and P. De Hert, “European Law Enforcement and US Data Companies: A Decade of Cooperation Free from Law,” in F. Fabbrini, E. Celeste and J. Quinn (eds.), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (London: Hart, 2021), 157–172.

³⁵ F. Spiezia, “International Cooperation and Protection of Victims in Cyberspace: Welcoming Protocol II to the Budapest Convention on Cybercrime” (2022) 23 *ERA Forum* 4.

³⁶ Council of Europe, *Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY*, T-CY(2014) 16, December 3, 2014, 3; Council of Europe, *Report of the Transborder Group for 2013*, T-CY(2013)30, November 5, 2013, 3; Koops and Goodwin, “Cyberspace, the Cloud,” 57; M. O’Floinn, “It Wasn’t All White Light before Prism: Law Enforcement Practices in Gathering Data Abroad, and Proposals for Further Transnational Access at the Council of Europe” (2013) 29 *Computer Law & Security Review* 611.

³⁷ Koops and Goodwin, “Cyberspace, the Cloud,” 57. Subsequently, interested stakeholders (such as Google, Paypal, etc.) and experts were invited to discuss the report at a June 3, 2013 hearing in the Council of Europe (O’Floinn, “It Wasn’t All White Light before Prism,” 611).

³⁸ Koops and Goodwin, “Cyberspace, the Cloud,” 10.

³⁹ T-CY Guidance Note No. 3, Transborder Access to Data (Article 32), T-CY(2013)7E; T-CY Guidance Note No. 10, Production Orders for Subscriber Information, T-CY(2015)16.

⁴⁰ See, for example, P. de Hert and A. Aguinaldo, “Cybercrime Convention-Based Access to Personal Data Held by Big Tech: Decades of Council of Europe’s Greenlighting Codified in a New Protocol,” in H. Matsumi, D. Hallinan, D. Dimitrova, E. Kosta and P. de Hert (eds.), *Data Protection and Privacy: In Transitional Times*, Computers, Privacy and Data Protection, vol. 15 (Oxford: Hart, 2023), 185–213.

and loosens the interpretation and application of Article 32 CC not only by providing scenarios that supposedly do not circumvent the abovementioned points but also by not providing an explicit prohibition for domestic determination concerning these important points.

On the other hand, Guidance Note No. 10 on domestic production orders concerns both computer data and subscriber information. Based on Article 18 CC, computer data production orders can be sent only to persons within the territory of the issuing party, while subscriber information production orders can be sent only to service providers providing services in the territory of the issuing party. With regard to subscriber information, Guidance Note No. 10 expands the Convention's definition by making it likewise applicable to all internet protocol (IP) addresses, some of which are traditionally considered traffic data due to their non-static nature. Subscriber information production orders can also be issued to service providers regardless of their location and/or registration as long as their services are provided in the territory of the issuing party. Hence, Guidance Note No. 10 provides a creeping effect in expanding the coverage of domestic production orders for subscriber information. The same expansion applies to computer data production orders wherein service providers can be recipients thereof as long as they are located in the territory of the issuing party and regardless of where the data is located as long as they have access and control.

8.5 STRUCTURE OF THE 2021 PROTOCOL

We saw that the T-CY gave an additional mandate to an ad hoc expert subgroup to draft an additional protocol to the Convention after accepting a first report in 2012.⁴¹ The work on the Second Additional Protocol began in June 2017 and should have been finished by the end of 2019.⁴² It was, however, only on November 17, 2021, in celebration of the twentieth anniversary of the CC, that the Committee of Ministers of the Council of Europe adopted the Second Additional Protocol to the Convention on enhanced cooperation and disclosure of electronic evidence.

The new protocol is meant to clarify matters on transnational access to electronic evidence and is supposed “to set out, among other things, a clearer framework and stronger safeguards for existing practices of transborder access to data and safeguards, including data protection requirements.”⁴³ It includes provisions for efficient and effective MLA and for direct transborder cooperation with providers, and it proposes a framework with safeguards for practices of transborder access to data.⁴⁴ Stronger judicial cooperation mechanisms, including direct cooperation with service providers, are placed at the fore to emphasize the necessary coordination of investigations between states.⁴⁵

⁴¹ O'Flóinn, “It Wasn't All White Light before Prism,” 611. The decision to move forward was based on the recommendations of the Cloud Evidence Working Group (2015–2017) and the earlier work of the Transborder Working Group (2012–2014). See also Council of Europe, *Legal Opinion on Budapest Cybercrime Convention: Use of a Disconnection Clause in the Second Additional Protocol to the Budapest Convention on Cybercrime*, April 29, 2019, www.coe.int/en/web/dlapil/-/use-of-a-disconnection-clause-in-the-second-additional-protocol-to-the-budapest-convention-on-cybercrime-1.

⁴² *Legal Opinion on Budapest Cybercrime Convention*; Council of Europe, *Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime: State of Play*, T-CY(2019)19, June 23, 2019, 2, <https://rm.coe.int/t-cy-2019-19-protocol-tor-extension-chair-note-v3/16809577ff>; De Hert, Parlar and Sajfert, “Guidance Note on Production Orders,” 335.

⁴³ S. Depauw, “Electronic Evidence in Criminal Matters: How About E-Evidence Instruments 2.0?” (2018) 8 *European Criminal Law Review* 62, 66; Tosoni, “Rethinking Privacy,” 17.

⁴⁴ *Legal Opinion on Budapest Cybercrime Convention*; De Hert, Parlar and Sajfert, “Guidance Note on Production Orders,” 335; Seger, “E-Evidence and Access,” 40.

⁴⁵ Spiezia, “International Cooperation,” 4.

The Second Additional Protocol relaunches the “applicative sphere of the basic Convention, confirming its centrality” in the procedures of international cooperation vis-à-vis crimes committed in cyberspace.⁴⁶ It does so through its four chapters with a total of twenty-five articles, namely, common provisions (Ch. 1), measures for enhanced cooperation (Ch. 2), conditions and safeguards (Ch. 3) and final provisions (Ch. 4).

Chapter 2 is the biggest chapter of the Second Additional Protocol. It contains different measures of enhanced cooperation that could apply in the absence of an existing treaty between the parties involved and on the basis of uniform or reciprocal legislation. This entire chapter is composed of five sections that provide different measures such as direct cooperation with providers and entities in other parties (s. 2), procedures enhancing international cooperation between authorities for the disclosure of stored computer data (s. 3), procedures pertaining to emergency mutual assistance (s. 4) and procedures pertaining to international cooperation in the absence of applicable international agreements (s. 5), such as the use of video conferencing and joint investigation teams.

Chapter 3 entails the conditions and safeguards concerning data protection and privacy. It provides the scope, purpose, legal parameters and remedies that could be made available to a party affected by the enforcement measures provided in the Protocol.

8.6 ACCESS TO DOMAIN NAME INFORMATION AND SUBSCRIBER INFORMATION (ARTS. 6 AND 7)

The first measures of enhanced cooperation introduced by the Protocol pertain to requests for domain name registration information (Art. 6) and for disclosure of subscriber information (Art. 7). For both measures, contracting parties ought to enact or adopt legislative and other measures to enable their authorities to request and to permit an entity in another party’s territory to provide domain name registration services and/or disclose subscriber information. The Protocol provides also what information a production order shall contain.

Timely access to these two sets of data (domain name registration information and subscriber information) is imperative in most criminal investigations.⁴⁷ On the one hand, the drafters recognize that criminals often create and exploit domains for malicious and illicit purposes.⁴⁸ Historically, domain name registration information is publicly accessible, but access to it lately has proven difficult due to increasing restrictions.⁴⁹ Thus, an effective and efficient framework is necessary, such as direct cooperation with domain name registration service providers that also considers restrictions existing in domestic law or the limitations on data protection grounds that the Second Additional Protocol provides.

⁴⁶ Ibid.

⁴⁷ In providing the legal framework for direct cooperation with providers or other entities for domain name registration information and subscriber information, the *Explanatory Report to the Convention on Cybercrime* (para. 73) explains:

The procedure also acknowledges the current model of internet governance which relies on developing consensus-based multistakeholder policies. These policies are normally based on contractual law. The procedure set out in this article aims to complement those policies for the purposes of this Protocol, that is, for the purpose of specific criminal investigations or proceedings. Obtaining the domain name registration data is often indispensable, as a first step for many criminal investigations and to determine where to direct requests for international co-operation.

⁴⁸ Ibid., para. 74.

⁴⁹ Ibid.

On the other hand, subscriber information is the most often sought information in criminal investigations vis-à-vis cybercrimes and other crimes where electronic evidence is needed.⁵⁰ The Protocol follows the definition of subscriber information as traditionally defined in Article 18, §3 CC.⁵¹ Subscriber information is considered to be less intrusive data because it does not pertain to the private lives and daily habits of the individuals concerned;⁵² however, it is traditionally understood to concern various types of information about a service's usage and the user thereof, as well as what is available on the basis of the service agreement or arrangement concerned.⁵³ This notwithstanding, the *Explanatory Report* notes that information needed to identify a subscriber can include IP address information, that is, information on the IP address used when the account was created, the most recent log-on IP address or the log-on addresses used at a specific time. However, some state parties classify this as traffic data instead. Thus, reservations on this account are allowed.⁵⁴

It is important to further note that Article 7 of the Second Additional Protocol broadens the limited scope of Article 18 CC,⁵⁵ and establishes “a complementary mechanism that would enable more effective cross-border access to information needed for specific criminal investigations or proceedings.”⁵⁶ Two requirements should, however, be met to effectuate disclosure: first, the service provider is physically present in the other party; second, the data is in the service provider's possession or control.⁵⁷

8.7 ENABLING DIRECT COOPERATION VIS-À-VIS DOMAIN NAME REGISTRATION AND SUBSCRIBER INFORMATION IS APPLAUDABLE BUT REMAINS QUESTIONABLE

Considering the abovementioned, we could highlight at least six points in the legal framework that legitimize direct cooperation between law enforcement authorities and providers or entities vis-à-vis digital evidence. First, there is the central idea of establishing a procedure allowing direct cooperation between law enforcement authorities and service providers in a territory of

⁵⁰ Ibid., paras. 23, 92.

⁵¹ Art. 18, para. 3 CC states:

For purposes of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: the type of communication service used, the technical provisions taken thereto, and the period of service; the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

⁵² If one further delves into the *Explanatory Report to the Convention on Cybercrime*, one could read in para. 177:

In principle, it refers to any information held by the administration of a service provider relating to a subscriber to its services. Subscriber information may be contained in the form of computer data or any other form, such as paper records. As subscriber information includes forms of data other than just computer data, a special provision has been included in the article to address this type of information. “Subscriber” is intended to include a broad range of service provider clients, from persons holding paid subscriptions, to those paying on a per-use basis, to those receiving free services. It also includes information concerning persons entitled to use the subscriber's account.

⁵³ Ibid., paras. 179, 180.

⁵⁴ Ibid., para. 93.

⁵⁵ Specifically, Article 18 of the Convention applies when a service provider is “in the territory” of the issuing party (see Art. 18, para. 1.a of the Convention) or “offering its services” in the issuing party (see Art. 18, para. 1.b of the Convention).

⁵⁶ *Explanatory Report to the Convention on Cybercrime*, para. 94.

⁵⁷ Ibid., para. 99.

another party to obtain domain name registration and subscriber information.⁵⁸ This expands the scope and coverage of Article 18 CC, which was seen to be an incomplete solution.⁵⁹ This procedure admittedly builds on the Report and Conclusions of the Cloud Evidence Group as well as Guidance Note No. 10 issued in 2017, as well as being a response to the alleged shortcomings of the current MLA framework on transborder access to digital evidence especially in urgent situations.⁶⁰ Mutual legal assistance is not completely disregarded, as direct cooperation does not encompass all forms of data. It is limited to types of data that are believed to be less intrusive. Thus, one could observe a direct proportional relationship between how intrusive a type of data is and the strictness of the enforcement mechanism involved to obtain it. Any other data outside domain name registration and subscriber information, such as traffic data, content data or metadata, necessitates more complex mechanisms such as government-to-government cooperation as provided in Articles 8 to 10 of the Protocol, or traditional MLA.

Second, although direct disclosure mechanisms are limited, there is a widened scope of the new competences. While subscriber information is said to follow the definition, stated earlier, in Article 18 CC, the new Protocol contemplates all forms of IP address equally as subscriber information. This stretches what constitutes “subscriber information” because dynamic IP addresses are traditionally considered “traffic data” due to their dynamic nature and being already intrinsically produced and entangled in the communications themselves.⁶¹ While this provision is subject to reservations, contracting parties have unbridled discretion to enable wider definitions of subscriber information in their domestic legislation. Further, this highlights the problematic lack of standardized delineation of data. Thus, it increases the potential risks and the lack of effective guarantees that data subjects will be exposed to when law enforcement authorities can practically access more than they are entitled to due to the difficulties encountered in delineating and classifying data.⁶²

Third, the provisions on direct cooperation enable parties to adopt the necessary measures for service providers found in their respective territories to respond to orders issued, which may include minimizing legal obstacles or bureaucracies to execute said orders.⁶³ There ought to be legal certainty that service providers will not incur legal liability for the sole fact of good faith compliance with an order.⁶⁴ Moreover, relevant provisions mention the possible inclusion and/or exclusion of data protection and human rights obligations but not necessarily the service provider’s exemption from legal liability due to good faith compliance.⁶⁵ We remain critical, however, because direct cooperation ultimately results in a paradigm shift from cooperation between authorities to one between authorities and private entities that ultimately do not have the same human rights obligations states have.⁶⁶ An unnecessary burden is then shifted to service

⁵⁸ Ibid., para. 1.

⁵⁹ Ibid., para. 94.

⁶⁰ See Boulet and Hernanz, “Cross-Border Law Enforcement Access,” 12.

⁶¹ De Hert, Parlar and Sajfert, “Guidance Note on Production Orders,” 327, 334.

⁶² See for discussion T. Wahl and C. Riehle, “News – European Union” (2018) 3 *European Criminal Law Association’s Forum (EUCrim)* 162; C. Warken, “Classification of Electronic Data for Criminal Law Purposes” (2018) 4 *EUCrim* 226, 229.

⁶³ *Explanatory Report to the Convention on Cybercrime*, para. 100.

⁶⁴ This is without prejudice, however, to other liabilities for reasons other than complying with the other. Ibid., para. 100.

⁶⁵ Ibid.

⁶⁶ The same is happening with the e-Evidence Regulation the European Union adopted in 2023: Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191/118 (e-Evidence Regulation). V. Mitsilegas, “The Privatisation of Mutual Trust in Europe’s Area of Criminal Justice: The Case of e-Evidence” (2018) 25 *Maastricht Journal of European and Comparative Law* 263, 264; see also S. Tosza, “Internet Service Providers as Law Enforcers and Adjudicators: A Public Role of Private Actors” (2021) 43 *Computer Law & Security Review* 43.

providers – regardless of size or architecture – to incur additional costs just to keep up with multiple jurisdictions or otherwise drive them out of existing markets.⁶⁷

Fourth, the scope of criminal offenses for which direct cooperation can be resorted to is unbridled. There is no limitation as to the seriousness of the criminal proceedings involved, for which direct cooperation is necessitated. This proves problematic in terms of costs and efficiency as a service provider can exhaust itself trying to respond to a high volume of orders for all sorts of crimes. Worse, there is the lack of any double criminality requirement that opens the usage of direct cooperation to abuse. It can be resorted to regardless of whether a crime is not criminalized or not punished in the same way in another country.⁶⁸

Fifth, the provision gives the option to a contracting party (when it is a receiving party) to require notification simultaneously if an order is sent to a service provider found in its territory (Art. 7, §5.a). There is also the option for the service provider to consult the receiving party on certain circumstances. Nonetheless, these notification and consultation procedures are discretionary. In connection to this, there is also room for a contracting party to instruct a service provider not to disclose information based on grounds provided for in Articles 25, §4 and 27, §4 CC (§5), but this should not be counterintuitive to the objective of Article 7, which is to remove barriers and to provide for more efficacious procedures for cross-border access to digital evidence in criminal matters.⁶⁹

These discretionary notification and consultation procedures resonate with the initial recommendations of the G8 in 1999 to put in place a mandatory notification requirement (*Principles on Transborder Access to Stored Computer Data*).⁷⁰ Concerns over breaches of other states' sovereignty caused by investigations on their respective territories presumably led the G8 to conclude this document.⁷¹ Nonetheless, notification is discretionary only in the Protocol and would depend on the decision of the contracting parties themselves. Therefore, there is an open window for a contracting party to have an informed decision in the process in general on the direct cooperation between law enforcement authorities and service providers found in the contracting party's territory.

Sixth, the entire framework on direct disclosure of subscriber information is bereft of any operationalization of data protection and/or human rights considerations. Although the Protocol later provides certain conditions and safeguards applicable to all stated measures, it merely scratches the surface by focusing on personal data; it still lacks other important human rights considerations such as defense rights, notification to the data subject and so on.

Even if a notification is required between involved states, and the requested state can be involved in the direct disclosure of data, there is nothing that factors in the data protection

⁶⁷ Hill, "Problematic Alternatives," 4; see also Tosza, "Internet Service Providers," 43.

⁶⁸ Electronic Frontier Foundation (EFF), European Digital Rights (EDRI), Association for Civil Rights (ADC), Derechos Digitales, Elektronisk Forpost Norge (EFN), IPANDETEC, Karisma Foundation, OpenMedia, Panoptykon Foundation, R3D: Red en Defensa de los Derechos Digitales, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), SonTusDatos and TEDIC, *Joint Civil Society Response to Discussion Guide on a 2nd Additional Protocol to the Budapest Convention on Cybercrime*, T-CY(2018)16, June 28, 2018, 7 and 20, www.eff.org/files/2018/08/02/globalcoalition-civilsociety-t-cy_201816-final.pdf.

⁶⁹ *Explanatory Report to the Convention on Cybercrime*, para. 21. In light of this, Art. 25, §4 CC states that "mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation," while Art. 27, §4 mainly allows refusal to assist if the subject offense is political in nature or the execution of the request is "likely to prejudice its sovereignty, security, ordre public or other essential interests." In other words, the requested state party determines the grounds by which it can refuse assistance as it may define in its own domestic framework.

⁷⁰ G8, *Principles on Transborder Access to Stored Computer Data*, October 1999, www.coe.int/t/dgi/legalcooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/24%2008%20Principles%20on%20Transborder%20Access%20to%20Stored%20Computer%20Data_en.pdf; Osula, "Remote Search and Seizure," 348; D. S. Wall, *Crime and Deviance in Cyberspace* (London: Routledge, 2017), 530.

⁷¹ Osula, "Remote Search and Seizure," 348.

obligations that are quintessential to the protection of the data subject itself, for example notification prior to processing. Thus, we consider it necessary to amend the Protocol to take into account these considerations.

8.8 COMPELLING SERVICE PROVIDERS TO PRODUCE STORED SUBSCRIBER INFORMATION AND TRAFFIC DATA (ARTS. 8 AND 9)

Drafters of the Protocol acknowledge that, while rapid and easier transborder access to digital evidence is necessary, a party is not able to use all of its enforcement mechanisms with regard to its domestic orders in another party's territory. Hence, certain procedures ought to be available. This includes situations where a provider cannot or does not want to disclose the information required. Aside from open channels of communication, resort to enforcement as provided by Article 8 of the Protocol and/or MLA is available.

Contracting parties ought to enact and adopt legislative measures to enable law enforcement authorities to request and permit orders to be submitted to another party for the purpose of compelling a service provider in the latter's territory to produce specified and stored subscriber information and traffic data (Art. 8). In relation to this, the Second Additional Protocol provides another provision that allows expedited disclosure of stored computer data in an emergency (Art. 9).

What is contemplated in Article 8 is an "order" to compel service providers⁷² located in another party.⁷³ The requested state must "give effect" to such an order. As to what "giving effect" means, the requested party shall be able to give effect in its territory to the order issued by the requested party by compelling the service provider to provide or surrender the required information.⁷⁴ This "giving effect" is subject to time limits, wherein the requested party ought to make reasonable efforts to process requests and have the service provider served within forty-five days after receiving all the required information and thereafter order the service provider to produce the subscriber information and traffic data within twenty days and forty-five days, respectively.⁷⁵

It should be mentioned that, as is the case in direct cooperation with providers, in compelling a service provider to provide either subscriber information or traffic data, the scope of criminal offenses to which it applies is unbridled. Further, the provider should be physically present in the territory of the other party to make this possible.⁷⁶ This is different from what was provided earlier in the Guidance Note on this matter, wherein domestic production orders are interpreted to allow issuance against service providers for subscriber information as long as they provide services to the territory of the issuing state.⁷⁷ For the purposes of the Protocol, a contractual relationship will not suffice. In other words, if a provider offers services to the other party but does not have a physical presence in that party's territory, then the provision is inapplicable. Further, in compelling to provide the needed information, the mechanism requested by the requesting party should apply.⁷⁸

As regards the expedited disclosure of stored computer data in an emergency vis-à-vis the twenty-four/seven network of points of contact under Article 35 CC (Art. 9 of the Second

⁷² This is defined as "any legal process that is intended to compel a service provider" to provide the subscriber information and/or traffic data (*Explanatory Report to the Convention on Cybercrime*, para. 126).

⁷³ It does not suffice that there is a contractual relationship with a company in a contracting party but without being physically present (*Explanatory Report to the Convention on Cybercrime*, para. 128).

⁷⁴ See §2 of the proposed provision; *Explanatory Report to the Convention on Cybercrime*, para. 129.

⁷⁵ *Ibid.*, para. 139.

⁷⁶ *Ibid.*, para. 128.

⁷⁷ See Council of Europe, *Guidance Note No. 10: Production Orders for Subscriber Information (Article 18 Budapest Convention)*, T-CY(2015)16, March 1, 2017.

⁷⁸ *Explanatory Report to the Convention on Cybercrime*, para. 129.

Additional Protocol), there was a conscious choice from the drafters to enable the parties to expeditiously obtain specified stored computer data in emergencies. This need for maximum expedited cooperation “may arise in a variety of emergency situations, such as in the immediate aftermath of a terrorist attack, a ransomware attack that may cripple a hospital system, or when investigating e-mail accounts used by kidnappers to issue demands and communicate with the victim’s family.”⁷⁹ In such cases, MLA can be facilitated through twenty-four/seven networks as provided in Article 35 CC.⁸⁰ This is without prejudice to other forms of cooperation available to the parties. In relation to this, the *Explanatory Report* provides that the use of twenty-four/seven networks may prove more advantageous than MLA due to the higher plausibility that requests shall be timely addressed and effectuated.⁸¹

8.9 “GIVING EFFECT TO ORDERS” FOR EXPEDITED PRODUCTION MAY FAIL EVEN BEFORE IT BEGINS

We observe that the foregoing provisions are heavily inspired by the concept of the European Investigative Order (EIO) and, more specifically, the European Preservation and Production Orders (under the EU e-Evidence Regulation) for digital evidence. These latter orders uncannily copy the EIO, which is thought to be an advanced (and expedited form) of MLA by allowing orders to be issued between requesting/issuing and requested/executing states without additional hurdles against their execution – shifting from a request-based to a demand-based system altogether.⁸² It forgoes the traditional utilization of central authorities and designates issuing and executing authorities instead.⁸³ Also, time limits are in place for expediency.⁸⁴

These are all the same features found in Article 8 of the Second Additional Protocol. Nonetheless, one cannot expect that what works for the EU with the EIO framework and the e-Evidence Regulation would work similarly for the Council of Europe. Indeed, in the EU, the legal framework is quite different and cross-border cooperation (e.g. in the context of the EIO) is based on the

⁷⁹ Ibid., para. 148.

⁸⁰ As para. 151 of the *Explanatory Report to the Convention on Cybercrime* states, this article permits parties to cooperate to obtain computer data in emergency situations using as a channel the 24/7 Network established by Article 35 of the Convention. The 24/7 Network is particularly well suited for handling the time-sensitive and high priority requests envisioned under this article. The 24/7 Network is staffed with points of contact who, in practice, communicate rapidly and without the need for written translations and are in a position to effectuate requests received from other parties, whether by going directly to providers in their territory, soliciting assistance from other competent authorities or going to judicial authorities, should that be required under the party’s domestic law. These points of contact can also advise requesting parties on questions they might have regarding providers and electronic evidence collection, for example by explaining the domestic law that must be satisfied to obtain evidence. Such back-and-forth communication enhances the requesting party’s understanding of the domestic law in the requested party and facilitates smoother acquisition of needed evidence.

⁸¹ *Explanatory Report to the Convention on Cybercrime*, para. 150.

⁸² Like what is provided herein, the EU e-Evidence Regulation involves expedited procedures as regards subscriber information, traffic data and so on while time limits, streamlined processes and the like, overall, reinforce and strengthen cooperation among law enforcement authorities and service providers, regardless of where the latter may physically be located. See M. A. Aguinaldo, *East Meets West: Development of Mutual Legal Assistance in Criminal Matters between and within the Association of Southeast Asian Nations and the European Union* (Baden-Baden: Nomos, 2020), 442. Directive 2014/41/EU of the European Parliament and of the Council of April 3, 2014 regarding the European Investigation Order in criminal matters, [2014] OJ L 130, May 1, 2014, Art. 1(1) defines the EIO as a “judicial decision which has been issued or validated by a judicial authority of a member state to have one or several investigative measures carried out in another member state to obtain evidence.”

⁸³ Directive on the EIO, Art. 2.

⁸⁴ Ibid., Art. 12.

principle of mutual recognition, which requires a high level of mutual trust.⁸⁵ This principle does not exist within the Council of Europe and those which may be signatories to the Second Additional Protocol. Not every state party has the same level of human rights protection. In fact, this lack of harmonization was enabled by the CC itself. As the Report of the Commissioner for Human Rights of the Council of Europe mentions, the Convention has three limitations vis-à-vis human rights and data protection: (1) the Convention's human rights clause is limited to procedural law; (2) there are conflicting applications in different national legal systems; and (3) there is "the so-called contentious provision on cross-border pulling of data by authorities."⁸⁶ We can look specifically at the EU member states, which are divided in their implementation and domestic application of EU data protection laws and policies: some are performing really well, while others are not. Unless the Council of Europe pushes for either approximation or harmonization of laws and thereafter adopts the same principle of mutual recognition among its member states, actualization of Article 8 might fail to protect what matters even before it actually begins.

8.10 POWERS TO USE EMERGENCY MLA PROCEDURES (ART. 10 OF THE PROTOCOL)

Article 10 of the Protocol provides for emergency MLA. Emergency as defined in Article 3, para. 2c, pertains to a situation "in which there is a significant and imminent risk to the life or safety of a natural person." The requesting party must be able to demonstrate through facts the existence of such an emergency and the assistance sought in response to said emergency. Moreover, both the requesting and the requested parties need to be on the same page that such an emergency exists. Significantly, whatever conditions are provided by the law of the requested party or by existing mutual legal assistance treaties (MLATs), including grounds for refusal, also apply to emergency MLA requests made under the Protocol.⁸⁷

The definition of emergency contemplated herein is lesser in scope compared to Article 25(3) CC, in which requests for mutual assistance may be made by expedited means of communications in urgent circumstances that do not rise to the level of emergency as defined: these are less urgent as they relate to "ongoing but non-imminent risks to life or safety of persons, potential destruction of evidence that may result from delay, a rapidly approaching trial date, or other types of urgencies."⁸⁸ Emergency MLA herein necessitates action on a "rapid expedited basis," including rapidly expediting the obtaining of judicial orders compelling a provider to produce data and equally rapid service of the order on the provider.⁸⁹ Any delays from the subject provider should not, however, be considered a delay of the authorities.

8.11 NEWLY CREATED POWER TO USE EMERGENCY MLA PROCEDURES MAY BE PROBLEMATIC IN CERTAIN SITUATIONS

Emergency MLA has been one of the proposals made by civil society organizations vis-à-vis the Protocol. Mainly against direct access to service providers, these organizations have pushed for

⁸⁵ There is "renunciation of an executing state of any control upon the grounds that motivate the request for evidence of the issuing state because the executing state can trust that the requesting authorities have checked the legality, necessity, and proportionality of the measure requested." See Aguinaldo, *East Meets West*, 423.

⁸⁶ Hayes et al., "The Law Enforcement Challenges," 47.

⁸⁷ *Explanatory Report to the Convention on Cybercrime*, para. 173.

⁸⁸ *Ibid.*, para. 172.

⁸⁹ *Ibid.*, para. 174.

reforms to be made instead on existing MLA systems.⁹⁰ They propose the establishment of emergency MLA procedures, wherein there is a mechanism for countries to “access the data in foreign countries necessary to prevent an emerging life-threatening situation, but also provide an opportunity to create strong privacy protections for this process.”⁹¹

These proposals have been duly integrated, but at the same time they created a set of problems. When the Protocol simultaneously offers both emergency MLA and direct access, emergency MLA can be just a white elephant. There is no clear delineation or proscription that prevents law enforcement authorities from pursuing direct access altogether instead of MLA. If one refers to Article 7, contracting state parties themselves have the autonomy to delineate types of data and define the legislative measures that allow for direct disclosure. This can, of course, include “emergency situations.” Thus, direct disclosure can be pursued equally in emergency situations, which would allow authorities to prevent additional channels and go direct to the source (i.e. service providers) to respond in emergency cases.

Assuming *arguendo* that MLA remains the general method of cross-border access to digital evidence, emergency MLA on its face lacks definite criteria, standards or procedure as regards the needed protection and promotion of human rights and data protection –notwithstanding the explicit mention by the T-CY that data protection and human rights are of primordial consideration. Conversely, these standards remain largely dependent on state action on a national level. What is lacking is a narrow and operationalized definition of what constitutes an emergency as well as a procedure to be followed so that said mechanism would not be abused.⁹²

8.12 THE SECOND ADDITIONAL PROTOCOL HAS STRONG POTENTIAL, BUT ALSO (FOUR) FLAWS

In view of the previously summarized developments, at least four additional issues can be identified. First, it is interesting how the T-CY supposedly was all-inclusive and implored stakeholders such as civil society, data protection groups and so on to participate, while encouraging participation and consultation during the drafting process. However, such inclusivity was questionable. Some civil society organizations narrated a different experience altogether. While they were given the chance to speak during the July 2018 Octopus conference and to raise their reservations toward the proposed Second Additional Protocol, they allege that it was difficult to be detailed as they are excluded from the drafting process.⁹³ It would be better if these stakeholders were given the real opportunity to be part of the drafting process, to flesh out the needed details and to ascertain that they are truly heard, by having their respective inputs integrated formally into the drafting and/or amendment process.

Second, nongovernmental organizations (NGOs) are wary of the lack of a sufficient framework toward the protection of human rights and data privacy with respect to direct access between law enforcement authorities and service providers.⁹⁴ In drafting the Second Additional Protocol, the T-CY vowed to consider rule of law standards. In fact, explicit mentions about data protection and fundamental human rights are scattered in all of the Second Additional Protocol documents. There is, nonetheless, a clear need to provide a definite and

⁹⁰ Rodriguez, O'Brien and Fernandez, “Behind the Octopus.”

⁹¹ *Joint Civil Society Response*, 7.

⁹² For comments of civil society organizations on an effective emergency MLA framework, see *Joint Civil Society Response*, 7.

⁹³ Rodriguez, O'Brien and Fernandez, “Behind the Octopus,” 2.

⁹⁴ *Ibid.*

delineated framework that ensures data protection and human rights obligations. The European Data Protection Board (EDPB) has recommended further amendments:

Provisional text of provisions on direct disclosure of subscriber information and on the giving effect to orders from another Party for expedited production of data, by laying down procedural conditions for access to personal data, may already impact on the level of protection of personal data and may also need to be amended in order to ensure the operational application of appropriate data protection safeguards.

The EDPB considers that specific provisions on data protection safeguards shall reflect key principles and in particular lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. These principles are also in line with the Council of Europe modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+), to which many Parties to the Convention on Cybercrime are also Party.⁹⁵

There should have been stronger data protection and fundamental human rights considerations with respect to the security of data processing involved. While the articles on direct disclosure of subscriber information and giving effect to orders require certain levels of security and authentication requirements vis-à-vis data processing, the EDPB's advice was correct to develop further requirements and specification in this regard. Rightly put, "ensuring that the necessary means are put in place so that the personal data are disclosed and communicated in a secure environment with the means to ensure the authenticity of documents is key for achieving the objective of a swift gathering of electronic evidence in compliance with fundamental rights."⁹⁶

As regards the security of data processing, the EDPB encouraged the T-CY to consider, "as a specific data protection safeguard, a mechanism for the notification without delay of data breaches that could seriously interfere with the rights and freedoms of data subjects. Personal data breaches could indeed potentially have a range of significant adverse effects for individuals concerned."⁹⁷

Third, the limitations and options provided in the Second Additional Protocol are decorative at best. With operationalization mainly hinging on national legislation, state players have unbridled discretion. Definition and delineation of data is an example. Emergency MLA provisions are another. Emergency MLA was inserted as a sort-of response to the suggestions of civil society organizations while retaining direct disclosure, which the same organizations are adamantly against. The article on giving effect to orders is technically just expedited MLA. However, by providing at the same time emergency MLA, direct disclosure of subscriber information and expedited disclosure of stored computer data using a twenty-four/seven network, cost-benefit analysis would dictate that there is no point for a law enforcement authority to choose questionably longer processes. Instead, law enforcement authorities would be more motivated to opt for direct disclosure by adjusting domestic legislation in its favor, rendering the other proposed articles unused, inutile and unappealing. Speaking in economic terms, direct disclosure is the superior good among all the available mechanisms provided by the Protocol because it would involve the least effort on the part of state players, albeit it might be burdensome to the private entities themselves.

Fourth, there is the obvious lack of provisions involving jurisdiction, albeit it could affect state interests and defense rights considerations. This is quite unsettling because direct disclosure of

⁹⁵ European Data Protection Board (EDPB), "EDPB Contribution to the Consultation on a Draft Second Additional Protocol to the Council of Europe Convention on Cybercrime (Budapest Convention)," November 13, 2019, <https://rm.coe.int/edpbcontributionbudapestconvention/t68098d940>.

⁹⁶ *Ibid.*, 5.

⁹⁷ *Ibid.*

subscriber information without considering where the service provider and/or data may be located has jurisdictional repercussions that the Council of Europe has been evading discussion of since the Guidance Notes. The Council of Europe puts the cart before the horse by jumping outright to specificities that allow law enforcement authorities almost unbridled access to digital evidence without adequate frameworks to protect human rights and data protection obligations. Herein it is not an issue of where the contracting parties or the members of the drafting groups can easily agree with each other; rather, it is the importance of addressing first the right foundations or rudiments in respect to cross-border access and transborder exchange of digital evidence. Jurisdiction, as is well known, has been at the crux of the issue of cross-border access to digital evidence. Without settling this important matter, the efforts made presently by the Council of Europe are grounded on unstable foundations that are susceptible to question and uncertainty. Thus, if the Council of Europe is keen to influence international law and policy as regards digital evidence in criminal matters, it ought to prioritize issues such as jurisdiction.

Based on the abovementioned observations, one could have been hopeful about the potential of the Protocol, but it fell flat. Its final provisions do consider comments coming from the different stakeholders to address the missing links, but the Council of Europe was still not brave enough to confront and settle each one. If the Council of Europe were not afraid to truly set the standard, to be specific in the standards and parameters that ought to put all contracting parties in line vis-à-vis cross-border access and transborder exchange of digital evidence, there could be room for further clarity and efficacy without necessarily disavowing the needed protection of data privacy and other fundamental human rights.

8.13 CONCLUSION: THE COUNCIL OF EUROPE SHOULD MOVE IN THE RIGHT DIRECTION WITHOUT LOSING SIGHT OF KEY NON-NEGOTIABLES

This chapter discussed the developments within the Council of Europe as regards cross-border exchange and transborder access to digital evidence in criminal matters. Particular focus was given to the adoption of the Second Additional Protocol. Prior to its adoption, the practice of direct cooperation between law enforcement authorities and service providers without the proper legal framework became common knowledge. To legitimize and legalize the practice, certain developments were seen on domestic, regional and international levels. The Council of Europe resorted to formation of expert groups and meetings, and to the extent of soft law instruments such as the Guidance Notes, to expand, legitimize or even radicalize unilateral transborder access to digital evidence, as well as reinforce direct cooperation with service providers. The Second Additional Protocol toned down some radical interpretations of the Guidance Notes one way or another through integration of certain standards, and allegedly considered input from other stakeholders. However, it still has its flaws, including the incompleteness of its protective safeguards against the risk of abuse from unilateral practices. There are still issues and concerns that the Council of Europe need to iron out. These include issues on jurisdiction as well as operationalizing data protection provisions and conditions that uphold the needed protection for fundamental human rights and data privacy. As correctly observed by Clough, in relation to “[t]he alternative of an additional Protocol to the *Convention*, specifying minimal procedural protections does not address the underlying problem if it applies only to a limited number of countries and/or is subject to reservations by countries.”⁹⁸

⁹⁸ J. Clough, “A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation” (2014) 40 *Monash University Law Review* 698, 711.

The Council of Europe has pushed the envelope on what is allowed and has been the enabling forum for law enforcement authorities to get what they supposedly need to counter crimes involving digital evidence. However, we do not live in a Machiavellian society in which the ends justify the means taken. Indeed, we are all in favor of changing the rules of the game if necessary, but without losing sight of non-negotiables such as data protection and fundamental human rights. Further, it does not suffice that commitments to these are mentioned. Motherhood statements at the end of the day are just motherhood statements. These non-negotiables ought to be operationalized and followed, especially in an organization where harmonization is almost nonexistent. Loose ends ought to be tied up as regards long-running issues on sovereignty, jurisdiction and so on, and these should serve as the foundations and rudiments of cross-border access to digital evidence. Thus, much work still needs to be done. We do not reserve this alone for the Council of Europe. Hence, these forums should make conscientious decisions that do not solely push efficacy and efficiency forward in criminal prosecutions and investigations but likewise find balance with competing values, rudiments and norms.

PART II

Digital Evidence and the Cooperation of Service Providers
in EU Criminal Investigations

Digital Evidence in Criminal Matters

Belgian Pride and Prejudice

*Sem Careel and Frank Verbruggen **

9.1 SETTING THE SCENE

9.1.1 *General Approach to the Collection of Digital Evidence*

It is a truth universally acknowledged that digital evidence is crucial for criminal investigations and trials. Not only do many criminal offences take place online but e-evidence is also increasingly decisive for traditional ‘offline crimes’. Although the digitisation of its criminal justice system is a tortuous and slow process, small and connected Belgium has not completely missed the e-train. Starting in 2000, it introduced or amended plenty of provisions in the Belgian Code of Criminal Procedure (CCP)¹ that take the particularities of digital evidence into account. The 2016 Internet Investigatory Powers Act² – slightly amended in 2019 after the Constitutional Court found parts of it unconstitutional³ – and the 2022 Data Retention Act⁴ provided the most recent legislative updates of the procedural cybercrime framework.

Several provisions and investigative measures explicitly address evidence in a digital form. The CCP contains provisions dealing with, for instance, overt searches of data stored in an information technology (IT) system⁵ and covert searches of such an IT system.⁶ The procedural regime for the seizure of data retrieved from an IT system also differs from the general provisions

* English translations of legal provisions used in this chapter do not have an official character, but were made by the authors. We thank Helena Severijns, Ruben Van Herpe and Dr Sofie Royer for their comments and valuable insights. All errors are our own.

¹ Code d’Instruction Criminelle of 17 November 1808 (Belgian Code of Criminal Procedure), *Moniteur belge* (MB) 27 November 1808.

² Loi portant des modifications diverses au Code d’instruction criminelle et au Code pénal, en vue d’améliorer les méthodes particulières de recherche et certaines mesures d’enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales (Internet Investigatory Powers Act), 25 December 2016, MB 17 January 2017; see, e.g., V. Franssen, ‘The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level’ (2017) 4 *European Data Protection Law Review* 534–542. For a more detailed analysis, see C. Forget, ‘Les nouvelles méthodes d’enquête dans un contexte informatique : vers un encadrement (plus) strict?’ (2017) 66–67 *Revue du droit des technologies de l’information* 25–52; V. Franssen and S. Tosza, ‘Vers plus de droits pour le justiciable sur internet? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l’information’, in V. Franssen and A. Masset (eds.), *Les droits du justiciable face à la justice pénale* (Limal: Anthemis, 2017), 205–249; and C. Conings and S. Royer, ‘Verzamelen en vastleggen van digitaal bewijs in strafzaken’ (2017) 4 *Nullum Crimen* 311–338.

³ Cour constitutionnelle (Belgian Constitutional Court), 6 December 2018, No. 174/2018.

⁴ Loi relative à la collecte et à la conservation des données d’identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (2022 Data Retention Act), 20 July 2022, MB 8 August 2022.

⁵ Art. 39bis CCP.

⁶ Art. 90ter CCP.

on seizure in criminal procedure.⁷ Article 46sexies CCP further contains the separate legal basis for online infiltration by law enforcement authorities (LEAs), that is, entering into contact with certain suspects in an internet environment, using a fictitious identity if that proves necessary. Moreover, the Belgian government has strongly advocated and supported EU initiatives in the field of e-evidence.⁸

Belgian law does not contain an explicit definition of ‘digital evidence’. However, deduced from the definition of ‘data’ in legislative documents,⁹ e-evidence can be defined as evidence consisting of data that has been stored, processed and transmitted in an IT system.¹⁰

The political enthusiasm cannot mask the enormous difficulties faced by Belgian LEAs. Several police departments lack technical tools and manpower, and specialised forces (such as the Regional Computer Crime Units and the Federal Computer Crime Unit (FCCU)) remain extremely understaffed.¹¹ When different police forces and the judiciary are compared in relation to their digital capabilities, there are huge disparities, too. The budget-restrained federal police and judiciary as well as poorer local police zones lag behind the bigger and/or richer local police units who have taken the lead and invested in digitisation. This undermines the effectiveness of the overall law enforcement effort and legislative changes alone will not remedy that.

Belgian rules on evidence are very open and judges have only limited possibility to exclude evidence, even illegally gathered evidence.¹² Furthermore, in the eyes of the Court of Cassation, human and digital rights concerns in matters of e-evidence are more often than not outweighed by other interests at stake, such as effective crime-fighting. Successful human rights challenges always happened in the Constitutional Court, frequently because supranational case law had already settled the matter. The annulment of data retention laws provided the most prominent illustration.

9.1.2 Data Retention Obligations: Legal Framework, Practice and Challenges

9.1.2.1 Impact of CJEU Judgments

Over the past decade, Belgium, when amending its legislation to comply with judgments of the Court of Justice of the European Union (CJEU) and the Belgian Constitutional Court, has always held on to a general data retention obligation.¹³ In 2015, the Constitutional Court struck down the general data retention obligation in force at the time, explicitly referring to *Digital Rights Ireland*.¹⁴ The 2016 Data Retention Act¹⁵ tried to meet the requirements of the CJEU, but

⁷ Arts. 35–39bis and 89 CCP. Art. 39bis specifically addresses the seizure of data retrieved from an IT system.

⁸ An example is the outspoken position of the then Belgian Minister of Justice: see N. Nielsen, ‘EU Seeks Access to “Digital Evidence”’, EUObserver, 24 March 2016, <https://euobserver.com/rule-of-law/132811>.

⁹ M. Giacometti, ‘Collecte transfrontalière de preuves numériques selon le point de vue belge. La décision d’enquête européenne, un moyen approprié?’, in V. Franssen and D. Flore (eds.), *Société numérique et droit pénal. Belgique, France, Europe* (Brussels: Bruylant, 2019), 289; see also Section 9.2.1.1.

¹⁰ Giacometti, ‘Décision d’enquête européenne, moyen approprié?’, 290.

¹¹ J. Kerkhofs and P. Van Linthout, *Cybercrime 3.0* (Brussels: Politeia, 2019), 43.

¹² F. Verbruggen and C. Conings, ‘After Zigzagging between Extremes, Finally Common Sense? Will Belgium Return to Reasonable Rules on Illegally Obtained Evidence?’ (2021) 7(1) *Revista Brasileira de Direito Processual Penal* 273–310.

¹³ For a historical overview (up to 2019), see F. Coudert and F. Verbruggen, ‘Conservation des données de communications électroniques en Belgique : un juste équilibre?’, in V. Franssen and D. Flore (eds.), *Société numérique et droit pénal. Belgique, France, Europe* (Brussels: Bruylant, 2019), 245–266.

¹⁴ Cour constitutionnelle, 11 June 2015, No. 84/2015, B.6; see also Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and others* [2014] ECLI:EU:C:2014:2338.

¹⁵ Loi relative à la collecte et à la conservation des données dans le secteur des communications électroniques (2016 Data Retention Act), 29 May 2016, MB 18 July 2016.

the government struggled to do so, branding some of the criteria suggested by the CJEU pointless or impossible to implement.¹⁶ Belgian lawmakers insisted that they attempted to balance the right to privacy with the importance of data retention for criminal investigations, especially, but by no means exclusively, investigations concerning terrorism and child pornography. The idea still was to have data on communications in the past available once a criminal offence is discovered. The new Article 126 of the Act on Electronic Communications (ECA)¹⁷ therefore reinstated a general obligation to retain personal non-content data, but limited the access of authorities thereto and surrounded it with several safeguards.

In the aftermath of the *Telez* judgment,¹⁸ another request was filed with the Constitutional Court seeking annulment of the 2016 Act. The Court asked for several rulings from the CJEU,¹⁹ highlighting the positive obligation of states that are party to the European Convention on Human Rights (ECHR) to protect the fundamental rights of minors and other vulnerable persons as possible justification for general data retention.

In early October 2020, the CJEU answered these questions in *La Quadrature du Net*.²⁰ It reaffirmed that a general data retention obligation for service providers remains, in principle, prohibited under EU law. Nonetheless, the security concerns of member states were taken into account, if only to some extent. For instance, when a state is confronted with a serious threat to national security, temporarily requiring service providers to indiscriminately retain all metadata is permitted. The Court is also more flexible as regards the retention of what it deems less privacy-sensitive types of data, such as subscriber data and internet protocol (IP) addresses. Targeted retention of traffic and location data for the objective of combating serious crime is also not precluded. It is, however, mandatory that the scope of the latter is limited, inter alia, in time and in space. We do agree with the Belgian authorities that a geographical delineation seems difficult to operationalise in practice (the place of criminal offences often remains hard to predict) and is not really adequate for cybercrime. It is also not clear where the line between (criminal offences threatening) national security, serious crime and non-serious crime can be drawn.

The answers left the Constitutional Court without options and it annulled the 2016 Data Retention Act. It did so in a judgment of April 2021,²¹ merely by copy-pasting *La Quadrature du Net*. Moreover, the CJEU also told the Constitutional Court that it could not limit the temporal effects of a declaration of illegality in this matter. Temporarily maintaining the effects of the 2016 Act and continuing to impose data retention obligations was thus not an option.²² Therefore, after 28 June 2021 (the date of publication of the Constitutional Court's judgment), service providers in Belgium no longer had a general data retention obligation.

An Act to restore the obligation was adopted by Parliament in 2022. An earlier draft had already been heavily criticised.²³ With this 2022 Data Retention Act, the government is purporting to

¹⁶ Explanatory Memorandum, *Projet de loi relatif à la collecte et à la conservation des données dans le secteur des communications électroniques*, *Doc. Parl.*, Ch. repr., sess. ord. 2015–2016, No. 54-1567/001, pp. 4–23, especially 4 and 9–12.

¹⁷ *Loi relative aux communications électroniques* (Act on Electronic Communications), 13 June 2005, *MB* 20 June 2005.

¹⁸ Joined Cases C-203/15 and C-698/15, *Telez Sverige AB* [2016] ECLI:EU:C:2016:970.

¹⁹ *Cour constitutionnelle*, 19 July 2018, No. 96/2018.

²⁰ Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net* [2020] ECLI:EU:C:2020:791; see also Case C-623/17, *Privacy International* [2020] ECLI:EU:C:2020:790, Case C-746/18, *Prokuratuur* [2021] ECLI:EU:C:2021:152 and Case C-140/20, *G.D. v. Commissioner of An Garda Síochána* [2022] ECLI:EU:C:2022:258.

²¹ *Cour constitutionnelle*, 22 April 2021, No. 57/2021.

²² *La Quadrature du Net*, §§219–220.

²³ For instance by the Belgian Data Protection Authority in its advice of 28 June 2021, No. 108/2021, www.autoriteprotectiondonnees.be/publications/avis-n-108-2021.pdf.

incorporate the newest case law and the categorisations made by the CJEU, while obviously trying to stretch data retention to the maximum. The targeted retention based on geographical criteria,²⁴ for instance, probably covers large parts of – if not the entire – Belgian territory. Moreover, for access to data retained on that ground, serious crime is defined by referring to Article 88bis(1), para. 1 CCP and as a consequence covers all criminal offences punishable with at least one year's imprisonment.²⁵ Only rarely will this be a real hurdle for LEAs requesting access. It seems unlikely that such a broad interpretation of the concept of serious crime is what the CJEU had in mind. The 2016 Act already applied to publicly available telephony, internet access and internet email service providers as well as to operators of public electronic communications networks. Earlier amendments of the ECA to bring it in line with the Directive establishing the European Electronic Communications Code²⁶ resulted in the new data retention regime also applying to over-the-top (OTT) service providers.²⁷ Lastly, a first draft contained an obligation for service providers to build in a backdoor for when content data has been encrypted, which received severe criticism from security experts, privacy activists and providers²⁸ and consequently no longer appears in the final text. The 2022 Data Retention Act nevertheless still contains some limitations to the freedom of encryption (Section 9.3.2).²⁹

9.1.2.2 Unlawful Retention: Admissible Evidence and Redress

The data retained under the 2016 Data Retention Act could be accessed by judicial authorities, under the conditions of Articles 46bis and 88bis CCP. Since the Act has been annulled, the question arises what the fate of the obtained evidence will be. This requires a twofold analysis.

First, evidence will be considered as illegally gathered under Belgian criminal procedural law if it has been obtained by LEAs (or the person reporting the criminal offence) (1) by committing an offence; (2) in violation of a rule of criminal procedure; (3) in violation of the right to privacy; (4) in breach of the rights of defence; or (5) in violation of the right to human dignity.³⁰ Unlawful retention seems to fall at least within the third category. Unlawfully retained data therefore constitutes illegally gathered evidence.³¹

Second, illegally gathered evidence will not necessarily be excluded. Article 32 Preliminary Title CCP (PT CCP) provides that such evidence can be declared void in a criminal procedure, but only (1) if the law explicitly envisages nullity as the sanction, or (2) if the reliability of the

²⁴ Arts. 126/1-126/3 ECA (Arts. 9–11 2022 Data Retention Act).

²⁵ Art. 127/1(1) read together with 127/1(4) ECA (Art. 13 2022 Data Retention Act). Serious crime in that context also includes the gravest violations of the Code de droit économique (Code of Economic Law), 28 February 2013, *MB* 29 March 2013 and the infringements of Arts. 14–15 Regulation (EU) 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (Market Abuse Regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, [2014] OJ L173/1, 12 June 2014 or provisions enacted on the basis or in execution of these articles.

²⁶ Directive 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code, [2018] OJ L321/36, 17 December 2018.

²⁷ Examples of OTT service providers are WhatsApp, Skype, Viber, Signal and so on.

²⁸ See GEC Admin, 'Open Letter: 107 Organizations and Cybersecurity Experts Call on the Belgian Government to Halt Legislation to Undermine End-to-End Encryption', Global Encryption Coalition, 28 September 2021, www.globalencryption.org/2021/09/open-letter-48-organizations-and-cybersecurity-experts-call-on-the-belgian-government-to-halt-legislation-to-undermine-end-to-end-encryption/; M. Verbergt, 'Groen en PS nemen afstand van af luisterwet', *De Standaard*, 1 December 2021, www.standaard.be/cnt/dmf20211130_98129127.

²⁹ Art. 107/5 ECA (Art. 3 2022 Data Retention Act).

³⁰ Cour de cassation (Belgian Supreme Court), 23 March 2004, No. P.04.0012.N, ECLI:BE:CASS:2004:ARR.20040323.24; R. Verstraeten, *Handboek strafvordering*, 5th ed. (Antwerp: Maklu, 2012), 984–1001.

³¹ Cour de cassation, 11 January 2022, No. P.21.1245.N, ECLI:BE:CASS:2022:ARR.20220111.2N.1.

evidence is affected, or (3) if using the evidence would be contrary to the right to a fair trial. To assess the third ground, the judge must take into account all elements of the case, including the way in which the evidence was gathered.³² The judge can, *inter alia*, take one or more of the following circumstances into consideration (the first being of particular importance): whether the unlawful action by the authorities was intentional or in gross disregard of the interests of the accused and their right to a fair trial; the gravity of the offence vis-à-vis the gravity of the unlawful action; the fact that the illegally gathered evidence concerns only the material element of the offence (the existence of an offence, as distinct from the guilt of the defendant); the impact of the illegality on the protected right; and the purely formal character of the rule that was broken.³³

With the *WebMindLicenses* judgment in mind,³⁴ the Constitutional Court had also asked the CJEU whether previously retained data could still be used if Belgian legislation were found to be incompatible with EU law.³⁵ In *La Quadrature du Net* and *Prokuratuur*,³⁶ the CJEU left it to the procedural autonomy of member states to establish the procedural consequences of retention or access contrary to EU law. These domestic rules, however, have to meet the principles of equivalence and effectiveness. As regards the latter principle, the CJEU points out that the objective of national rules on the admissibility and use of evidence is to prevent unlawful evidence from unduly prejudicing a suspect. The CJEU continues: ‘That objective may be achieved under national law not only by prohibiting the use of such information and evidence, but also by means of national rules and practices governing the assessment and weighting of such material, or by factoring in whether that material is unlawful when determining the sentence.’³⁷ Nonetheless, the principle of effectiveness requires national courts to exclude unlawful evidence when they are of the view that a party is not in a position to comment effectively on evidence pertaining to a field of which the judges have no knowledge and is likely to have a preponderant influence on the findings of fact.

Belgian legislation does not foresee nullity in the case of unlawful data retention. The resulting evidence can therefore be excluded under Article 32 PT CCP only if the illegality threatens the reliability (which is unlikely) or the right to a fair trial. After the 2015 and 2021 annulments of the data retention legislation by the Constitutional Court, the highest national courts indeed have confirmed this principle: evidence obtained through unlawful retention does not have to be excluded, and Article 32 PT CCP has to be applied.³⁸ Belgian judgments do additionally take the recent jurisprudence of the CJEU into account, but mostly still declare the evidence (certainly evidence gathered before the formal annulment of the 2016 Data Retention Act) admissible on the basis of Article 32 PT CCP. In Belgium, evidence already had to be disregarded when a party was not able to comment effectively on it.³⁹ That part of the CJEU judgments therefore does not seem to be problematic. Article 32, applying to violations of both EU law and domestic law, is certainly in line with the principle of equivalence. More interesting

³² Cour de cassation, 23 March 2004.

³³ Cour de cassation, 23 March 2004; Cour de cassation, 2 March 2005, No. P.04.1644.F, ECLI:BE:CASS:2005:ARR.20050302.10; Cour de cassation, 23 September 2008, No. P.08.0519.N; Cour de cassation, 4 April 2023, No. P.22.1730.N.

³⁴ Case C-419/14, *WebMindLicences kft.* [2015] ECLI:EU:C:2015:832.

³⁵ Cour constitutionnelle, 19 July 2018. See F. Verbruggen, S. Royer and H. Severijns, ‘Reconsidering the Blanket-Data-Retention-Taboo, for Human Rights’ Sake?’, European Law Blog, 1 October 2018, <https://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/>.

³⁶ *La Quadrature du Net*, §§222–228 and *Prokuratuur*, §§41–44.

³⁷ *La Quadrature du Net*, §225 and *Prokuratuur*, §43.

³⁸ Cour de cassation, 19 April 2016, No. P.15.1639.N, ECLI:BE:CASS:2016:ARR.20160419.3; Cour de cassation, 11 January 2022; Cour constitutionnelle, 22 April 2021, B.24.3.

³⁹ Cour de cassation, 25 September 2002, No. P.02.0954.F, ECLI:BE:CASS:2002:ARR.20020925.11.

is the question of whether this provision meets the principle of effectiveness. In that regard, the question arises whether necessarily one of the three aforementioned consequences suggested by the CJEU has to be attached to data retention and/or access contrary to EU Law. New questions to the CJEU to provide clarification on this are highly desirable, but the Court of Cassation has refused to ask them, suggesting that application of Article 32 PT CCP without any doubt suffices to meet the effectiveness of EU data protection law as required by the CJEU.⁴⁰

Another possibility of judicial redress is to bring a civil action for damages against the state on the basis of Article 1382 of the Belgian Civil Code⁴¹ if the unlawful retention, access or use caused harm. To our knowledge, there have not been any such cases yet.

9.2 TERMINOLOGY AND CATEGORISATIONS

9.2.1 Data

9.2.1.1 Terminology

The Belgian federal lawmaker is traditionally reluctant to use statutory definitions. Hence, the CCP does not contain a general definition of ‘data’. The Explanatory Memorandum regarding the first Belgian statute on cybercrime⁴² defined data as ‘any representation of information in a form suitable for the storage, processing and transmission in an IT system’.⁴³ This very broad concept was meant to be as technology-neutral as possible.⁴⁴ The practical relevance of this definition is, however, limited to substantive criminal law, for instance to clarify the constituent components of cybercrimes like computer-related forgery.⁴⁵ The lack of a general definition does not seem to create any problems on a domestic level.

9.2.1.2 Categorisation

The CCP contains different investigative measures involving data, from which the following categorisation can be distinguished:

- identification of a subscriber or common user of a service consisting of transmitting signals through electronic communications networks or permitting users to obtain, receive or spread information through such a network, identification of the electronic means of communication used and identification of these services (= subscriber and identification data);⁴⁶
- gathering of traffic data of electronic means from which or to which electronic communications are or have been performed and localisation of the origin or destination of electronic communications (= traffic and location data);⁴⁷
- overt search of data in an IT system and covert interception/searching of not publicly available communication or data of an IT system (= content data).⁴⁸

⁴⁰ Cour de cassation, 29 March 2022, No. P.22.0078.N, ECLI:BE:CASS:2022:ARR.20220329.2N.15.

⁴¹ [Ancien] Code Civil (Belgian Civil Code), 21 March 1804, MB 3 September 1807.

⁴² Loi relative à la criminalité informatique (Belgian statute on cybercrime), 28 November 2000, MB 3 February 2001.

⁴³ Explanatory Memorandum, Projet de loi relatif à la criminalité informatique, *Doc. Parl.*, Ch. repr., sess. ord. 1999–2000, No. 50-0213/001, p. 12.

⁴⁴ Explanatory Memorandum, *Doc. Parl.*, Ch. repr., sess. ord. 1999–2000, No. 50-0213/001, p. 12.

⁴⁵ See Art. 210bis CC.

⁴⁶ Art. 46bis(1), para. 1 and para. 2, second indent CCP.

⁴⁷ Art. 88bis(1) CCP.

⁴⁸ Arts. 39bis and 90ter(1) CCP; see also Art. 88ter CCP.

This distinction is based on the sensitivity of the data concerned and it also determines the competent authority. Under Belgian law, a distinction has to be made between an investigation led by a public prosecutor and a judicial inquiry led by an investigating judge. At the end of the latter, an intervention of an investigation supervision court (*juridiction d'instruction*), mostly the council chamber (*chambre du conseil*), is required. A large majority of criminal investigations are led by the public prosecutor. However, judicial inquiries remain relevant for the most serious cases and when investigative measures forming serious infringements of human rights are required.⁴⁹ The investigating judge has indeed more extensive competences, but can also order all investigative measures that can be ordered by the public prosecutor.⁵⁰ For certain investigative measures, the public prosecutor can ask the investigating judge to order or allow those measures without opening a judicial inquiry (the so-called mini-instruction).⁵¹ The investigating judge then can grant or refuse that measure. The judge who grants the measure can choose to send the file back to the prosecutor after it has been performed, but may also open a judicial inquiry and take it out of the hands of the prosecutor. If hereafter we state that the intervention of an investigating judge is required, we mean that both a mini-instruction and a judicial inquiry are possible. If a full judicial inquiry is required, we will explicitly indicate this.

Identification data is the least sensitive and thus has to be delivered upon the request of the prosecutor (Article 46bis CCP). For traffic and location data, which is already more intrusive, an intervention of the investigating judge is in principle needed (Article 88bis CCP). The difference between both types of data is not always crystal clear, which is regrettable since this is crucial to determine the competent authority.⁵² Regarding highly sensitive content data, cooperation regarding interception of it and covert search of (the content of) an IT system in principle requires a judicial inquiry (Article 90quater(2) CCP). Nonetheless, cooperation with an overt search in an IT system requires an intervention of the investigating judge, but not necessarily a judicial inquiry.⁵³

Login information (e.g. usernames) can be considered identification data. Dynamic IP addresses can be classified as identification data or traffic and location data. When LEAs know the exact point in time when the dynamic IP address was used, the investigative measure under Article 46bis can be used.⁵⁴ When LEAs do not know this and, as a result, have to request at which point in time a certain computer has had contact with other non-specified computers, they should resort to Article 88bis CCP.⁵⁵ Decryption keys are regarded as a means to facilitate searches of IT systems and interception rather than as a type of data.⁵⁶ The same conclusion applies to passwords. Unread emails contain all three types of data. Depending upon the drafting progress, draft emails can also contain any or all of the types of data. Chat rooms and communication in the context of online games mainly include content data. Lastly, machine-to-machine data does not seem to fit into any of the categories.

⁴⁹ J. Fermon, F. Verbruggen and S. De Decker, 'The Investigative Stage of the Criminal Process in Belgium', in E. Cape, J. Hodgson, T. Prakken and T. Spronken (eds.), *Suspects in Europe: Procedural Rights at the Investigative Stage of the Criminal Process in the European Union* (Oxford: Intersentia, 2007), 30.

⁵⁰ Art. 56(1) CCP.

⁵¹ Art. 28septies CCP.

⁵² C. Conings, *Klassiek en digitaal speuren naar strafrechtelijk bewijs* (Mortsel: Intersentia, 2017), 304, para. 485 *et seq.*

⁵³ Art. 88quater CCP.

⁵⁴ 'Court of Appeal Ghent (Indictments Chamber) 26 May 2006' (2007) 4 *Nullum Crimen* 287; Explanatory Memorandum, *Projet de loi modifiant l'article 46bis du Code d'instruction criminelle*, *Doc. Parl., Sén., sess. ord.* 2005–2006, No. 3-1824/1, p. 5.

⁵⁵ Explanatory Memorandum, *Doc. Parl., Sén., sess. ord.* 2005–2006, No. 3-1824/1, p. 5.

⁵⁶ See Arts. 39bis(5), 88ter, 88quater and 90quater(4) CCP.

9.2.2 Service Providers

Initially, the cooperation duty under Article 46bis CCP applied to ‘operators of an electronic communications network’ and ‘providers of an electronic communications service’. The terminology was intentionally⁵⁷ the same as under the ECA, where these terms were further defined.⁵⁸ Companies that use an existing network infrastructure only to offer an application or software without transmitting information themselves, such as Yahoo!, were not electronic communications service providers under the ECA then.⁵⁹

In the 2011 *Yahoo!* judgment,⁶⁰ the Belgian Court of Cassation held that ‘provider of an electronic communications service’ under Article 46bis CCP should be interpreted as also *including* persons offering a service that allows their clients to obtain, receive or distribute information through electronic communications networks.⁶¹ Some commentators criticised the Court’s conclusion.⁶² In particular, the question can be asked whether the Court of Cassation’s interpretation was sufficiently foreseeable and in conformity with the principle of legality.⁶³ Nonetheless, the reasoning of the Court of Cassation is understandable in the light of the (Belgian) principle of conceptual autonomy of criminal law. This principle allows giving a certain unique meaning to a concept without being bound to terminology and interpretations in other branches of law.⁶⁴ The Court could therefore interpret this term more broadly than under the ECA.⁶⁵ Moreover, the definition by the Court of Cassation is in conformity with the definition of service providers under Article 1 of the Cybercrime Convention.⁶⁶

With the Internet Investigatory Powers Act, Parliament inserted the broad interpretation of the 2011 *Yahoo!* judgment into Articles 46bis, 88bis and 90quater(2) CCP. Article 39quinquies(1), inserted by the 2022 Data Retention Act, uses a similar wording. Now, the cooperation duties under these provisions apply to (1) operators of an electronic communications network and (2) any person, within the Belgian territory, providing or offering by any means a service consisting of signal transmission through an electronic communications network or enabling users to obtain, receive or distribute information through electronic communications networks. The latter category includes providers of an electronic communications service as well. Now covered under the new provisions are not only companies offering web services, such as Yahoo!, Google, Skype and Microsoft, but also services such as Facebook, Twitter, WhatsApp and Instagram.⁶⁷

⁵⁷ Explanatory Memorandum, *Doc. Parl.*, Sén., sess. ord. 2005–2006, No. 3-1824/1, p. 7.

⁵⁸ The current version of the ECA repeats verbatim the definitions of ‘electronic communications network’ and ‘electronic communications service’ used in the Directive establishing the European Electronic Communications Code.

⁵⁹ F. Verbruggen and K. De Schepper, ‘Ontsnappen space invaders aan onze pacmannen? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische dienstverleners’ (2013) 3 *Tijdschrift voor Strafrecht* 153.

⁶⁰ Yahoo! was prosecuted for refusal to cooperate under Art. 46bis CCP. This resulted in three judgments of the Court of Cassation, which is highly exceptional.

⁶¹ Cour de cassation, 18 January 2011, No. P.10.1347.N, ECLI:BE:CASS:2011:ARR.20110118.1.

⁶² See, for instance, N. Vandezande, ‘Yahoo! als operator of verstreker’ (2011) 2 *Auteurs en media* 220–223; Conings and Royer, ‘Verzamelen digitaal bewijs in strafzaken’, 321. See also the Conclusion of Advocate General M. De Swaef under Cour de cassation, 18 January 2011, ECLI:BE:CASS:2011:CONC.20110118.1.

⁶³ Franssen, ‘The Belgian Internet Investigatory Powers Act’, 539.

⁶⁴ See Cour de cassation, 27 March 1995, no. P.94.0135.N, *Arr.Cass.* 1995, 351 and Cour de cassation, 24 October 2012, No. P.12.1011.F.

⁶⁵ Verbruggen and De Schepper, ‘Ontsnappen space invaders aan onze pacmannen?’, 154–155.

⁶⁶ Council of Europe, *Convention on Cybercrime*, ETS No. 185, 23 November 2001; Franssen, ‘The Belgian Internet Investigatory Powers Act’, 539; Verbruggen and De Schepper, ‘Ontsnappen space invaders aan onze pacmannen?’, 154.

⁶⁷ Explanatory Memorandum, *Projet de loi relatif à l’amélioration des méthodes particulières de recherche et de certaines mesures d’enquête concernant Internet, les communications électroniques et les télécommunications*, *Doc. Parl.*, Ch. repr., sess. ord. 2015–2016, No. 54-1966/001, pp. 32–33.

Providers of OTT services would thus fall under this broad definition as well. The wording of the legislator is, however, not as general (and technology-neutral) as the definition of ‘service provider’ under the Cybercrime Convention.⁶⁸ According to the Court of Cassation, internet access providers (IAPs), which are a subcategory of internet service providers (ISPs), are among the addressees of the cooperation duty under Article 39bis(6) CCP (Section 9.3.3.5).

The Code of Economic Law (CEL) contains other terms and definitions which form the implementation of the Directive on electronic commerce.⁶⁹ A service provider is defined as any natural or legal person that provides an information society service.⁷⁰ Services of the information society cover mere conduit, caching and hosting services as defined in line with the Directive.⁷¹ Despite not being part of the CCP, these definitions can also be relevant in a criminal procedure since Article XII.20 CEL provides a cooperation duty for these service providers (Section 9.3.2). There are no recorded problems related to the coexistence of different terms at the national level because of the aforementioned conceptual autonomy of criminal law.

9.3 DOMESTIC COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

9.3.1 *Introduction*

9.3.1.1 Practical Importance

The cooperation of service providers has become a very common feature of domestic criminal investigations. The growing number of compensation payments to cooperating service providers reflects this tendency. The Report to the King attached to the 2016 Royal Decree concerning these compensation fees highlights that, despite a reduction of the compensation fees by 50 per cent in 2011 and 2013, government expenditure is again at the 2007 level owing to the increase of cases where cooperation is requested.⁷² Finally, statistics published by the Belgian Institute for Postal Services and Telecommunications (BIPT) show a growing number of cases where (retained) identification, traffic and/or location data was requested and provided to the competent authorities.⁷³

9.3.1.2 Territorial Scope of Application

Determining the territorial scope of application of a cooperation duty requires a threefold analysis. First, jurisdiction for the underlying offence (for which cooperation was requested) has to be established. Next, it needs to be assessed whether Belgian LEAs have procedural jurisdiction to issue an order to the service providers. Lastly, since failure to cooperate is considered a punishable act, the territorial applicability of Belgian substantive criminal law

⁶⁸ Franssen, ‘The Belgian Internet Investigatory Powers Act’, 540.

⁶⁹ Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on Electronic Commerce’), [2000] OJ L178/1, 17 July 2000.

⁷⁰ Art. L18, 3 CEL.

⁷¹ Art. XII.17–19 CEL.

⁷² Report to the King, Arrêté royal modifiant l’arrêté royal du 9 janvier 2003 déterminant les modalités de l’obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques, relatif aux tarifs rétribuant la collaboration, 8 November 2016, *MB* 22 December 2016.

⁷³ BIPT, ‘Statistics Data Retention 2018’, 1 October 2019, www.ibpt.be/operators/publication/statistics-on-data-retention-in-2018.

comes into play again. The rules to determine the territorial scope of both substantive criminal law and criminal procedure will hence be discussed next.

9.3.1.2.1 TERRITORIAL SCOPE OF APPLICATION OF SUBSTANTIVE CRIMINAL LAW. The general principle of territorial applicability of Belgian substantive criminal law can be found in Article 3 of the Criminal Code (CC):⁷⁴ Belgian criminal law applies to criminal offences committed on Belgian territory, regardless of the nationality of the perpetrator(s). However, legislation does not offer any specific guidelines to establish the place where a criminal offence has been committed. Therefore, case law and doctrine have adopted and standardly use the so-called theory based on the objective ubiquity criterion. On the basis of this theory, a criminal offence is deemed to be committed in any place where an objective constitutive component of that offence (partly or wholly) occurs.⁷⁵ The fact that only ‘objective constitutive components’, that is, elements of the *actus reus*, are taken into account means that the place where the perpetrator has formed their intent to commit an offence does not influence its localisation.

Moreover, domestic courts often consider themselves competent to rule on criminal offences committed in a foreign country that form an indivisible whole with criminal offences that are localised in Belgium under the objective ubiquity theory⁷⁶ or when an indivisible aspect or part of the criminal offence manifests itself in Belgium.⁷⁷ This broad interpretation can result in Belgian judges establishing competence when the more remote (material) effects of a criminal offence are located in Belgium.⁷⁸

9.3.1.2.2 LOCATION IN CRIMINAL PROCEDURE LAW. In principle, a state can force compliance with domestic laws only within its territory. Unilateral measures on other states’ territory are prohibited under the, still dominant, strict interpretation of international law and would violate a state’s sovereignty. That the Belgian LEAs do not have to physically enter foreign territory to execute the measure, but rather use (the threat of) a fine imposed by a Belgian criminal court, does not alter that.⁷⁹ The question is therefore when Belgian LEAs have procedural jurisdiction for a coercive measure. What are the relevant connecting factors in this regard?

Regarding (the search for) stored data, the traditional view in Belgium seems to be that the location of the data determines which state has jurisdiction.⁸⁰ This finds support in Article 31 of the Cybercrime Convention. In addition, Article 32 of the Cybercrime Convention includes

⁷⁴ Code pénal (Belgian Criminal Code), 8 June 1867, MB 9 June 1867.

⁷⁵ See, for instance, Cour de cassation, 23 January 1979, *Arr.Cass.* 1978–1979, 575; Cour de cassation, 14 November 2000, No. P.00.1231.N, ECLI:BE:CASS:2000:ARR.20001114.8; Cour de cassation, 26 May 2009, No. P.09.0438.N, ECLI:BE:CASS:2009:ARR.20090526.7; Cour de cassation, 7 June 2011, No. P.11.0172.N, ECLI:BE:CASS:2011:ARR.20110607.6.

⁷⁶ Cour de cassation, 24 January 2001, No. P.00.1627.F, ECLI:BE:CASS:2001:ARR.20010124.11.

⁷⁷ Verbruggen and De Schepper, ‘Ontsnappen space invaders aan onze pacmannen?’, 150.

⁷⁸ Verbruggen and De Schepper, ‘Ontsnappen space invaders aan onze pacmannen?’, 150; P. Van Linthout ‘Territoriale bevoegdheid in cyberspace’ (2009) 2 *Tijdschrift voor Strafrecht* 113. See also Cour de cassation 23 January 1979, *Arr.Cass.* 1978–1979, 575 and ‘Corr. Dendermonde 29 September 2008’ (2009) 2 *Tijdschrift voor Strafrecht* 111–112, where the judge considered himself to be competent since the victim of the hacking had opened his computer and had suffered the effects of the hacking in the judge’s jurisdiction. These elements were considered to form an indivisible whole with the acts committed by the defendant.

⁷⁹ K. De Schepper, ‘Cassatie bevestigt: Belgische gerecht kan rechtstreeks gegevens vorderen van Yahoo’ (2016) 7 *Rechtspraak Antwerpen Brussel Gent* 489.

⁸⁰ C. Conings, *Locating Criminal Investigative Measures in a Virtual Environment: Where Do Searches Take Place in Cyberspace*, B-CCENTRE Legal Research Report 2011–2014 (Leuven: Belgian Cybercrime Centre of Excellence for Training, Research & Education, 2015), 55, www.law.kuleuven.be/citip/en/research/projects/finalized/documents/B-CCENTRE-Research-Report-Legal_FINAL.pdf. In our view, the location of the data controller instead of the location of the data would make more sense as a connecting factor.

exceptions allowing direct cross-border access to stored data. Belgian law, however, goes further than the Convention (which does not prohibit this) when describing the competency for a cross-border network search.⁸¹ A network search means that the search of an IT system is expanded to other IT systems connected to the first system. Article 88ter, para. 4 CCP states: ‘if it becomes apparent that these data are not to be found on Belgian territory, they will only be copied. In that case, the investigating judge communicates this, without delay, to the Ministry of Justice, which notifies the competent authority of the respective State, if this state can be reasonably determined.’⁸² Apparently, the purpose of this notification is to allow the other state to verify whether or not the copied data has been lawfully obtained under its national laws.⁸³ Nonetheless, even if the evidence is labelled illegally gathered, this does not necessarily lead to exclusion (Section 9.1.2.2). The legislative objective is to exceptionally enable a unilateral trans-border network search in urgent cases or when the other state where the data is stored cannot be identified.⁸⁴ Since this exception also applies when the other state is not party to the Cybercrime Convention or not identifiable, the question arises whether it is compatible with the prohibition on unilateral extraterritorial investigative acts.⁸⁵

The location of the data is in principle also the connecting factor for the expedited preservation of data, as follows from Article 39quater CCP.⁸⁶ This provision addresses cross-border situations and describes these as situations where data is stored, processed or transmitted by means of an IT system located in the territory of another state. However, the procedure of Article 39quater(1) must not necessarily be followed. With the wording ‘notwithstanding the possibilities to cooperate directly with the foreign operators of electronic communications networks and providers of electronic communications services’ under this provision, Parliament wanted to provide a legal base for the forms of direct cooperation that exist in practice (Section 9.4.2.2).⁸⁷ Although not explicitly confirmed in Parliament or by case law (yet), this also leaves room to interpret the territorial scope of Article 39ter CCP as broadly as that of Articles 46bis, 88bis and 90quater(2) CCP, discussed later.⁸⁸ In conclusion, only when the data can be found in Belgium do the Belgian LEAs undeniably have jurisdiction to *force* service providers to cooperate with the expedited preservation of data or searches of IT systems and networks.

As regards the cooperation duty under Article 39bis(6) CCP (blocking access to data or websites), no territoriality issues have been recorded. The (vague) legal basis does not allow

⁸¹ Conings, ‘Klassiek en digitaal speuren’, 787.

⁸² Art. 88ter, para. 4 CCP. This provision is also applicable in the context of covert searches of an IT system (Art. 90quater, para. 5 CCP). In practice, these notifications only rarely take place.

⁸³ Explanatory Memorandum, *Doc. Parl.*, Ch. repr., sess. ord. 1999–2000, No. 50-0213/001, p. 24.

⁸⁴ Explanatory Memorandum, *Doc. Parl.*, Ch. repr., sess. ord. 1999–2000, No. 50-0213/001, pp. 24–25; D. Dewandeleer, ‘Misdrijven en strafonderzoek in de IT-context’, in *Themis 57 – Straf- en strafprocesrecht* (Bruges: die Keure, 2017), 150.

⁸⁵ This issue was also raised by the Belgian Council of State (*Doc. Parl.*, Ch. repr., sess. ord. 1999–2000, No. 50-0213/001 and 50-0214/001, pp. 45–49 and *Doc. Parl.*, Ch. repr., sess. ord. 2015–2016, No. 54-1966/001, p. 126). See the Case of the SS Lotus, *Fr v. Turk*, 1927 PCIJ (ser. A) No. 10 (Decision No. 9) (Permanent Court of International Justice). See also C. Conings and J. J. Oerlemans, ‘Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend’ (2013) 1 *Computerrecht: Tijdschrift voor informatica, telecommunicatie en recht* 27 and M. Corhay, ‘L’extension de la recherche dans un système informatique: Du droit belge à la Convention de Budapest sur la cybercriminalité’ (2020) 8 *Journal des tribunaux* 133–141.

⁸⁶ V. Franssen and O. Leroux, ‘Recherche policière et judiciaire sur internet : analyse critique du nouveau cadre législatif belge’, in V. Franssen and D. Flore (eds.), *Société numérique et droit pénal. Belgique, France, Europe* (Brussels: Bruylant, 2019), 173; see also S. Royer, *Strafrechtelijk beslag* (Bruges: die Keure, 2020), 120 *et seq.*

⁸⁷ Explanatory Memorandum, *Doc. Parl.*, Ch. repr., sess. ord. 2015–2016, No. 54-1966/001, p. 30.

⁸⁸ Franssen and Leroux, ‘Recherche policière et judiciaire sur internet’, 173–174.

determining a connecting factor, but, in practice, an order to cooperate under this provision always seems to be addressed to service providers established in Belgium (Section 9.3.3.5).

For the cooperation duties related to production orders (Articles 46bis and 88bis CCP) and the covert data interception measure (Articles 90ter–90quater CCP), the situation is rather complex. In two controversial cases (*Yahoo!* and *Skype*) of mixed situations (i.e. offences and probably suspects territorially linked to Belgium, but service providers not established in Belgium), Belgian jurisdiction has been interpreted broadly.

First, in the *Yahoo!* landmark case, one of the legal questions raised concerned the territorial scope of application of Article 46bis CCP (production order for identification data). *Yahoo!*, the defendant, was convinced that it could not be forced to cooperate since the company was headquartered in the USA, had no Belgian office and was thus not physically present in Belgium. The prosecuting authorities, however, argued that Article 46bis CCP was addressed to any provider offering targeted services in Belgium.

In a judgment of 1 December 2015 (the 2015 *Yahoo!* judgment),⁸⁹ the Court of Cassation confirmed the view of the prosecutor: any operator or service provider actively directing its economic activities to consumers in Belgium can be forced to cooperate with judicial authorities under Article 46bis CCP. No mutual legal assistance request to the state where the service provider is headquartered is required. Especially relevant, according to the Court, is that Article 46bis contains a coercive investigative measure that is limited in scope, such that execution of it does not require an intervention outside Belgian territory. The Court seemed of the opinion that the data should be brought to and will be received by LEAs in Belgium. Finally, the Court held that the refusal to cooperate (substantive criminal law) was committed at the location where the data has to be delivered, that is, in Belgium (procedural jurisdiction).

Second, in the *Skype* case,⁹⁰ a Belgian investigating judge ordered Skype to produce traffic and location data (Article 88bis CCP), and to intercept communication in Belgium between suspects (Article 90quater CCP). Skype was headquartered in Luxembourg, had no Belgian office and was thus not physically present in Belgium. The most notable difference from the previous case is the object of the investigative measure, the data requested being significantly more privacy-sensitive. Similarly to *Yahoo!*, Skype refused to cooperate, claiming that the investigating judge should resort to mutual legal assistance procedures. Moreover, Skype argued that it was unable to comply with the order owing to a conflict with Luxembourg law and the technical impossibility of intercepting communication. This led to criminal prosecution of Skype for failure to cooperate.

Again, Belgian courts endorsed the LEAs' position: Skype was convicted by an Antwerp criminal tribunal of first instance.⁹¹ This decision was later confirmed by the Antwerp Court of Appeal⁹² and the Court of Cassation.⁹³ The Court of Cassation ruled that Articles 88bis and 90quater(2) CCP do allow the investigating judge to order the cooperation of any operator of an electronic communications network and any provider of an electronic communications service actively directing its economic activities to consumers in Belgium regarding electronic communication carried out in Belgium. The Court continued that neither the place where the operator or provider is based nor the place where the infrastructure required to fulfil the request can be

⁸⁹ Cour de cassation, 1 December 2015, No. P.13.2082.N, ECLI:BE:CASS:2015:ARR.20151201.1.

⁹⁰ We discuss the *Skype* case before addressing the 2016 legislative amendments since the case concerns the cooperation duties under the old rules.

⁹¹ 'Corr. Antwerp 27 October 2016' 353 *Nieuw Juridisch Weekblad* 921.

⁹² 'Court of Appeal Antwerp 15 November 2017' (2018) 375 *Nieuw Juridisch Weekblad* 78.

⁹³ Cour de cassation, 19 February 2019, No. P.17.1229.N, ECLI:BE:CASS:2019:ARR.20190219.1.

located is relevant to determine Belgian jurisdiction. Finally, an operator or provider actively directing its economic activities to consumers in Belgium is subject to Belgian legislation and the cooperation duty does not require any intervention outside Belgian territory. Therefore, the Court of Cassation came to the conclusion that no mutual legal assistance request was needed and the investigating judge was not bound by foreign legislation. It is not entirely clear whether the Court meant, with such a general statement, that the domestic cooperation duty prevails over a duty of confidentiality under Luxembourg law.⁹⁴

From this case law, we can deduce that the active targeting of consumers for economic activities, that is, the place where services are offered, is considered to be a relevant connecting factor to establish jurisdiction to impose a cooperation duty, backed up by criminal sanctions for failure to cooperate. In the 2015 *Yahoo!* judgment, the Court of Cassation approved the decision of the Court of Appeal that by using a local domain name (www.yahoo.be) and the local language, publishing advertisements based on the location of its users and being accessible in Belgium for those users via, inter alia, a helpdesk and a customer complaint desk, Yahoo! was actively directing its economic activities towards Belgian consumers.⁹⁵ The question can be asked whether the reach of the domestic provisions has not been limited after the 2019 *Skype* judgment. In this judgment the Court of Cassation added that the investigating judge can order cooperation of any operator or provider actively directing its economic activities to consumers in Belgium regarding electronic communication carried out in Belgium. In the case at hand, the Belgian LEAs wanted to intercept communication in Belgium between suspects living within the Belgian territory and calling each other while they were on Belgian soil.⁹⁶ Does this mean that the location of the suspect and the location of the communication are also connecting factors, and, if so, are those two additional connecting factors alternative or cumulative? The judgment of the Court of Cassation unfortunately does not allow us to determine unequivocally which of these is the case.

As mentioned earlier (Section 9.2.2), the Internet Investigatory Powers Act has codified the Court of Cassation's 2011 *Yahoo!* judgment. In the Explanatory Memorandum, the government stated that the new provisions did not deal directly with the territoriality issue and that it was striving for a European legal framework to address this problem.⁹⁷ Indeed, only the 2011 *Yahoo!* judgment (concerning the personal scope of application) – and not the 2015 *Yahoo!* judgment (concerning the territorial scope of application) – was mentioned in the preparatory documents. This is, however, certainly not enough to conclude that Parliament rejected the 2015 and 2019 case law of the Court of Cassation.

Several authors argue that the new provisions still reflect a largely unilateral approach to the territoriality issue.⁹⁸ As the case law of the Court of Cassation still stands and Parliament has not explicitly rejected it, we are inclined to agree. The current wording of Articles 46bis, 88bis and 90quater(2) CCP combined with the judgments of the Court of Cassation allows us to establish a territorial link when services are actively targeted to Belgian consumers. Put simply, LEAs seem to be

⁹⁴ F. Verbruggen and S. Royer, 'Veroordeling Skype niet verbroken, vele vragen blijven onbeantwoord' (2018–2019) 37 *Rechtskundig weekblad* 1442; see also V. Franssen and M. Corhay, 'La fin de la saga Skype: Les fournisseurs de services étrangers obligés de collaborer avec la justice belge en dépit des possibilités techniques et de leurs obligations en droit étranger' (2019) 8 *Revue de droit commercial belge* 1020–1021.

⁹⁵ The Court might have been inspired by the CJEU's decision on how to determine whether a website is directed to (the consumer-inhabitants of) a certain country for international private law purposes (see Joined Cases C-585/08 and C-144/09, *Peter Pammer* [2010] ECLI:EU:C:2010:740, especially §93).

⁹⁶ Kerkhofs and Van Linthout, *Cybercrime* 3.0, 468.

⁹⁷ Explanatory Memorandum, *Doc. Parl.*, Ch. repr., sess. ord. 2015–2016, No. 54-1966/001, pp. 10–11.

⁹⁸ Franssen, 'The Belgian Internet Investigatory Powers Act', 540; P. Monville, M. Giacometti and L. Grisard, 'La collecte des preuves numériques en droit belge après l'arrêt de la Cour constitutionnelle du 5 décembre 2018' (2019) 9–10 *Revue de droit pénal et de criminologie* 1030; Franssen and Corhay, 'La fin de la saga Skype', 1022.

allowed to order any such service provider, irrespective of the location of its headquarters, establishments or the place where it stores its data, to cooperate and deliver the requested data without having to resort to mutual legal assistance.⁹⁹ Regarding subscriber data (and only subscriber data), it can be argued that this is in line with Article 18(1)(b) of the Cybercrime Convention.¹⁰⁰

In 2019, in the context of amendments regarding another provision (Article 46quater), the legislator explicitly stated that the 2016 amendments of Articles 46bis and 88bis CCP had also expanded their territorial scope.¹⁰¹ Such an approach whereby the legislator clarifies previous changes outside the scope of the legislative amendments should not be applauded. So, in our view, these remarks cannot be used to interpret the territorial scope of Articles 46bis and 88bis CCP. However, it is noteworthy that the 2019 lawmaker refers only to these provisions, but not to Article 90quater(2) CCP. Since 2016, the latter provision contains a cooperation duty for both the interception of data and the covert search of an IT system. While the current scope of the cooperation duty is suitably tailored to the interception of data (also a subject of discussion in *Skype*), it seems a bit odd to apply it to covert searches of an IT system. Especially since this would mean that the territorial connecting factor is different for overt searches of an IT system (Article 39bis CCP) compared to covert searches thereof.

A next question is whether the cooperation duty under Article 90quater(4) CCP has the same broad territorial scope as those of Articles 46bis, 88bis and 90quater(2) CCP (taking into account the remarks made in the previous paragraph). This provision contains a duty to provide information and a decryption duty in the context of the covert interception of data. The wording of the *Skype* and *Yahoo!* judgments has not been copied and pasted into this provision. Instead, this cooperation duty is addressed to ‘persons having special knowledge’. The Court of Appeal did rule, in the *Skype* case, that the company should organise itself technically so that the cooperation duty under Article 90quater(2) CCP can be complied with.¹⁰² This seemed to point in the direction that the scope of Article 90quater(2) and (4) CCP was similar, which would guarantee the *effet utile* of Article 90quater(2) CCP. A duty to cooperate with the interception of data without an information/decryption duty would indeed make the former less effective. On the other hand, this might be a too far-reaching interpretation not supported by a strict reading of Article 90quater(4) CCP. The Court of Cassation did not rule explicitly on this specific issue. Hence, the territorial scope of the cooperation duty under Article 90quater(4) CCP remains uncertain.

The cooperation duty that was added in 2022 regarding the future preservation of data (Article 39quinquies CCP) also adopts the wording of the 2011 *Yahoo!* judgment (Section 9.2.2). Again, reference is made solely to the 2011 *Yahoo!* judgment in the preparatory documents.¹⁰³ The territorial scope of this cooperation duty is thus still unclear, but we think that a similarly broad application to that under Articles 46bis, 88bis and 90quater(2) CCP would be condoned by the Court of Cassation.

⁹⁹ Franssen, ‘The Belgian Internet Investigatory Powers Act’, 539; Monville, Giacometti and Grisard, ‘Collecte des preuves numériques après l’arrêt du 5 décembre 2018’, 1030.

¹⁰⁰ See also Council of Europe, *T-CY Guidance Note #10 Production Orders for Subscriber Information (Article 18 Budapest Convention)*, 1 March 2017, 6; Franssen and Corhay, ‘La fin de la saga Skype’, 1016.

¹⁰¹ Explanatory Memorandum, Proposition de loi portant des dispositions diverses en matière pénale et en matière de cultes, *Doc. Parl.*, Ch. repr., sess. ord. 2018–2019, No. 54-3515/001, pp. 19–20.

¹⁰² ‘Court of Appeal Antwerp 15 November 2017’ (2018) 375 *Nieuw Juridisch Weekblad* 82–83.

¹⁰³ Explanatory Memorandum, Projet de loi relatif à la collecte et à la conservation des données d’identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, *Doc. Parl.*, Ch. repr., sess. ord. 2021–2022, No. 55-2572/001, p. 139.

9.3.2 Mandatory Cooperation

In domestic situations, mandatory cooperation appears to be the rule. The relevant provisions consider cooperation a ‘legal duty’ and include criminal penalties for service providers that are unwilling to cooperate with Belgian LEAs. There is no general legal basis for mandatory cooperation; the cooperation duty is outlined separately for each specific investigative measure.

Nonetheless, under Article XII.20 CEL, a more general cooperation duty can be found, the scope of which is, however, limited to service providers acting as an intermediary, defined earlier (Section 9.2.2). This provision requires those service providers to inform the LEAs of any presumed illegal activities or unlawful information provided by their clients and to provide, at the request of the competent LEAs, all information at their disposal that could be useful for the detection and identification of offences whereby they (unwillingly) acted as an intermediary.

Some more law enforcement-oriented authors deplore that this provision remains under-used.¹⁰⁴ Service providers falling under this cooperation duty are, however, excused only when their intervention is automatic and passive in nature, which means that the intermediary service provider has neither knowledge of nor control over the information stored or passed on.¹⁰⁵ Non-compliance with this mandatory form of cooperation can result in criminal penalties, namely a fine of up to 200,000 euros or up to 6 per cent of the annual turnover.¹⁰⁶

Data obtained through mandatory cooperation can in principle be used as evidence in court. To assess whether exclusion is required, the same steps as explained earlier (Section 9.1.2.2) need to be followed. These are: (1) is the evidence illegally gathered? And, if so, (2) should the evidence be excluded under Article 32 PT CCP? Since the service provider is often not involved in the criminal proceedings in which the evidence is used, there is rarely a possibility for them to challenge the admissibility before criminal courts. However, resorting to the procedure for lifting a seizure might be a solution (Section 9.3.4.2).

Not a lot of defences are available to the service provider to justify a refusal to cooperate. Besides a blunt refusal, standardised and meaningless replies are also considered refusal to cooperate.¹⁰⁷ The same goes for a slow or late reply: Articles 46bis(2) and (3), 88bis(2) and 90quater(2) CCP require service providers and operators to cooperate without delay (*en temps réel*) or at the point in time specified in the order. Without delay means after the minimal duration of time necessary for the execution of a proper performance, without interruption and using the appropriate amount of means and personnel.¹⁰⁸ Consciously or unconsciously postponing cooperation will also result in a punishable failure to cooperate.¹⁰⁹

A defence based on lack of technical means to deliver the requested data is not provided for under the legislation and was also not accepted in domestic case law.¹¹⁰ In *Skype*, the Court of Appeal ruled that the service provider should take the necessary technical and organisational measures to ensure that the cooperation duty (of Article 90quater(2) CCP) can be complied

¹⁰⁴ Kerkhofs and Van Linthout, *Cybercrime* 3.0, 178.

¹⁰⁵ Cour de cassation, 3 February 2004, No. P.03.1427.N, ECLI:BE:CASS:2004:ARR.20040203.3.

¹⁰⁶ Art. XV.118, 3 CEL read together with Art. XV.70 CEL.

¹⁰⁷ ‘Court of Appeal Antwerp 15 November 2017’, 82–83.

¹⁰⁸ Art. 1, 3 Arrêté royal déterminant les modalités de l’obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques (modalités de coopération RD), 9 January 2003, MB 10 February 2003.

¹⁰⁹ Monville, Giacometti and Grisard, ‘Collecte des preuves numériques après l’arrêt du 5 décembre 2018’, 1029; Explanatory Memorandum, *Doc. Parl.*, Ch. repr., sess. ord. 2015–2016, No. 54-1966/001, p. 34.

¹¹⁰ Monville, Giacometti and Grisard, ‘Collecte des preuves numériques après l’arrêt du 5 décembre 2018’, 1028; Franssen, ‘The Belgian Internet Investigatory Powers Act’, 540.

with.¹¹¹ A defence based on that argument will thus most likely be considered refusal to cooperate.¹¹² It is unclear whether this would mean that it is prohibited to offer communication software to Belgian customers if the provider does not retain the possibility to grant Belgian LEAs interception capacity. The question can also be asked whether such an obligation to create ‘backdoors’ would be compatible with EU law and human rights instruments. Defences based on the legislation of the service providers’ state of establishment (a duty of confidentiality) and on the freedom to provide services (Article 56 TFEU) were rejected by the Court of Appeal in the same case.¹¹³ Unfortunately, in its 2019 judgment the Court of Cassation did not provide more clarity on these three issues.¹¹⁴ It is even more unlikely that a defence based on the excessive costs of the operation would be upheld, especially since domestic law provides compensation of costs for cooperation duties under Articles 46bis, 88bis and 90quater(2) CCP (see also Section 9.3.1.1).¹¹⁵

However, under Belgian law, service providers refusing to cooperate can always try to invoke a state of necessity to justify their action and thus escape criminal liability. Necessity can justify criminal behaviour if the *prima facie* criminal behaviour was necessary to avert an imminent and serious danger to a good or interest (e.g. privacy) that one is obliged or entitled to look after.¹¹⁶ Moreover, refusal to cooperate would have to be the only reasonable way to safeguard said good or interest. Finally, the good or interest that the service provider would want to protect by refusing to cooperate has to be of higher or equal importance as the interest underlying the cooperation duty (e.g. the principle of truth-finding). This justification ground does not have a legal basis, but has been recognised by the Belgian Court of Cassation.¹¹⁷ To our knowledge, this ground of justification has not been successfully invoked by a service provider yet to escape criminal liability for refusal to cooperate. Nonetheless, in our view, states with far-reaching claims of jurisdiction (such as Belgium) have to take the laws of other (sovereign) states which have a closer connection with the suspect and/or service provider sufficiently into account. This is a consequence not just of the principle of (respect for) territorial sovereignty but also of the foreseeability dimension of the principle of legality in criminal law and the *comity* (or *comitas gentium*) logic underpinning mutual recognition between states with different legislations. Therefore, a legitimate justification raised by the service provider based on the laws of that jurisdiction could, in our opinion, be accepted to set aside the Belgian cooperation duty under this justification ground.¹¹⁸ A similar approach has also been followed by the EU under its e-Evidence Regulation.¹¹⁹

¹¹¹ ‘Court of Appeal Antwerp 15 November 2017’, 83. Art. 107/5(3) ECA (Art. 3 2022 Data Retention Act) states that encryption should not prevent the execution of a request made by LEAs to produce identification, traffic or location data.

¹¹² Franssen, ‘The Belgian Internet Investigatory Powers Act’, 540.

¹¹³ ‘Court of Appeal Antwerp 15 November 2017’, 82.

¹¹⁴ Verbruggen and Royer, ‘Veroordeling Skype niet verbroken’, 1442; Franssen and Corhay, ‘La fin de la saga Skype’, 1018.

¹¹⁵ Arts. 1–4 Annex modalities of cooperation RD.

¹¹⁶ A. Dierickx, ‘Over de (putatieve) noodtoestand’ (2007) 6 *Nullum Crimen* 395–403.

¹¹⁷ Cour de cassation, 13 May 1987, *Arr.Cass.* 1986–1987, 1203.

¹¹⁸ See also F. Verbruggen, ‘“Om af te sluiten, druk op Start”: Zesde rechter in Belgische Yahoozaak schaarst zich achter eerste’ (2014) 3 *Computerrecht: tijdschrift voor informatica, telecommunicatie en recht* 129–140. (Downloadable at Kluwer Navigator, www.navigators.nl/, 8.)

¹¹⁹ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191/118 (e-Evidence Regulation).

9.3.3 Overview of Existing Cooperation Duties

9.3.3.1 Brief Overview

Table 9.1 gives an overview of the most important cooperation duties.¹²⁰ Some ‘packet leaflet information’ may be useful. First, Belgian criminal law divides criminal offences into three subcategories, depending on their seriousness. From less serious to most serious, they are: contraventions/petty offences (*contraventions*), misdemeanours (*délits*) and crimes/felonies (*crimes*).¹²¹ Second, legal persons are also criminally liable in Belgium, but since they cannot serve prison sentences, the mechanism of Article 41bis CC must be applied. This provision explains how to determine the fine for legal persons and how to convert prison terms into fines.

9.3.3.2 Production Orders

The first type of mandatory cooperation are orders to produce identification/subscriber data (Article 46bis CCP) and traffic/location data (Article 88bis CCP).¹²² Service providers falling under the scope of both of these provisions have to assign one or more persons tasked with compliance therewith (called the Coordination Cell Justice).¹²³

Article 46bis CCP arguably covers all types of data allowing identification of the subscriber or common user. To gain access to identification data, a written and reasoned order is required in which special attention must be paid to proportionality in view of the right to privacy and subsidiarity in relation to other investigative measures.¹²⁴ According to the Court of Cassation, this requirement of a motivation should, however, not be interpreted too rigidly.¹²⁵ For minor offences (punishable with less than one year of imprisonment), the prosecutor or investigating judge can, however, only access data regarding the six months predating the decision.¹²⁶ The Belgian criminal justice system is notoriously slow, so federal prosecutor Kerkhofs and investigating judge Van Linthout consider that this is often too short for useful identification.¹²⁷

Access to traffic and location data mostly requires the intervention of an investigating judge.¹²⁸ When the offender has been caught in the act committing one of the offences listed under Article 9oter(2–4) CCP,¹²⁹ the public prosecutor can act without prior authorisation. Nevertheless, a confirmation by an investigating judge within twenty-four hours in principle remains necessary.¹³⁰ Article 88bis CCP is for instance used to obtain IP addresses of persons using a certain email address or service on the internet, to request internet traffic or to track a

¹²⁰ The CCP contains several other specific cooperation duties, for instance for postal operators to help with the interception of classical mail (Art. 46ter CCP) and for banking and credit institutions as well as virtual currencies service providers (Art. 46quater CCP).

¹²¹ See Art. 1 CC.

¹²² Similar provisions (Arts. 464/13 and 464/25 CCP) exist in the specific context of a criminal investigation regarding the execution of sentences (e.g. to trace fugitive convicted persons).

¹²³ Art. 2 modalities of cooperation RD.

¹²⁴ Art. 46bis(1), paras. 1 and 5 CCP. An oral order with subsequent written confirmation is possible in urgent situations.

¹²⁵ Cour de cassation, 29 March 2011, No. P.10.1755.N.

¹²⁶ Art. 46bis CCP.

¹²⁷ Kerkhofs and Van Linthout, *Cybercrime* 3.0, 292.

¹²⁸ Art. 88bis CCP.

¹²⁹ These provisions list the criminal offences of a certain gravity for which the covert data interception measure (Section 9.3.3.4) is possible. Examples are murder, trafficking in human beings, money laundering, genocide, crimes against humanity and the counterfeiting of money.

¹³⁰ Art. 88bis(1), para. 6 CCP (exceptions are listed under paras. 7–8). See also the limited competence of the public prosecutor under para. 9 (offences of cyberstalking).

TABLE 9.1 *Overview of cooperation duties*

Investigative measure	Legal basis	Type of data	Service providers addressed	Conditions	Possible sanctions if refusal
Production order	Art. 46bis CCP	Identification data	Broad (Section 9.2.2) + Banking and credit institutions, virtual currencies service providers, closed detention centres (and legal persons-subscribers)	To detect crimes and misdemeanours (not for petty offences) Written and reasoned decision (subsidiarity and proportionality!) Time constraints Ordered by public prosecutor	Fine of 800 to 240,000 euros*
Production order	Art. 88bis CCP	Traffic and location data (also live)	Broad (Section 9.2.2)	Serious indications of offences punishable with one year's imprisonment or more + measure necessary to establish truth Time constraints Written and reasoned decision (circumstances justifying measure, subsidiarity, proportionality and duration) Ordered by investigating judge (with some exceptions)	Fine of 800 to 240,000 euros
Search of IT system or network (provide information on operation/ accessibility of IT system or on way to make content accessible)	Art. 88quater (1) CCP	Content data	Any person deemed to have special knowledge (a) of the IT system or (b) of services used to secure or encrypt data	Over/covert search of IT system or network allowed Written and reasoned decision (circumstances justifying measure + sent to prosecutor) Ordered by investigating judge	(Also for hindering search): Fine of 800 to 240,000 euros When cooperation could have impeded execution of crime or misdemeanour or reduced consequences of those offences:
Search of IT system or network (operate IT system or search, make accessible, copy, block or delete data)	Art. 88quater (2) CCP	Content data	Any person deemed fit		

Interception of data and covert search of IT system	Art. 90quater (2) CCP	Content data	Broad (Section 9.2.2)	Required by the investigation + other investigative measures not sufficient to find truth + serious indications of offences listed under Art. 90ter (2-4) CCP Written and reasoned decision (facts justifying measure, reasons why necessary to reveal truth, scope, duration ...) Time constraints Requires in principle judicial inquiry (exceptions)	Imprisonment of 1-5 years and/or a fine of 4,000 to 400,000 euros For legal persons, a fine of 48,000 to 960,000 euros
	Art. 90quater (4) CCP	Content data	Any person deemed to have special knowledge (a) of means of the communication or IT system subject of the measure or (b) of services or applications used to protect, encode or encrypt data		
Blocking of access to data (website)	Art. 39bis(6) para. 3 CCP + 417/56 CC	Content data	IAPs + ... (scope not clear from judgment Cass.)	Lawful overt search in IT system Seizure of data carrier not desirable Copying of data not possible Ordered by public prosecutor	(only when data is related to some terrorist offences, non-consensual distribution of sexual content and child pornography) Fine of 1,600 to 120,000 euros

TABLE 9.1 (continued)

Investigative measure	Legal basis	Type of data	Service providers addressed	Conditions	Possible sanctions if refusal
Expedited preservation of data	Art. 39ter CCP	Data processed, stored or transmitted	Any person having the data in possession or under control	To detect crimes and misdemeanours (not for petty offences) Reasons to assume that data is particularly vulnerable to loss or modification Written and reasoned decision (scope, duration, criminal offence concerned ...) Ordered by officer of judicial police	(Also for modification or destruction of data or making data disappear) Fine of 800 to 240,000 euros
Future preservation of data	Art. 39quinquies CCP	Traffic and location data	Broad (Section 9.2.2)	Serious indications of offences punishable with one year's imprisonment or more Written and reasoned decision (scope, duration, criminal offence concerned ...) Ordered by public prosecutor	

* The nominal amount payable is 100 to 30,000 euros, but, to protect the fines against inflation, a surcharge of 700 per cent has to be added to criminal fines in Belgium ('décimes additionnels'), which means that 7 euros are added for each nominal euro of the fine, that is, each euro of the fine is multiplied by 8.

computer.¹³¹ The investigating judge has to state the duration for the future explicitly (a maximum of two months, with the possibility of renewal) and how far in the past LEAs can go back.¹³² Indeed, this provision covers not only the order to produce already stored data but also the real time interception of traffic and location data. There used to be time constraints (twelve, nine or six months, depending on the seriousness of the criminal offence) and additional guarantees for access to data which might endanger legal or medical privilege, but those provisions were annulled along with the rest of the 2016 Data Retention Act by the Constitutional Court in its 2021 judgment. Both guarantees were reinstated by the 2022 Data Retention Act.¹³³

9.3.3.3 Searches of an IT System

Article 88quater CCP contains two more cooperation duties in the context of searches of (data in) an IT system (e.g. a smartphone, a computer, the Global Positioning System (GPS) ...) or a network search. The authority competent to order the search does not necessarily have the authority to order cooperation with such a search. On the one hand, the officer of the judicial police or the public prosecutor is competent to order the overt search of an IT system, but every extension (to other systems) requires the intervention of an investigating judge.¹³⁴ Moreover, every other overt search of an IT system not falling under the previous provisions also requires an intervention of an investigating judge.¹³⁵ Before issuing the order, the investigating judge has to establish that the measure is necessary to reveal the truth and is proportionate. A covert search even requires a judicial inquiry (Section 9.3.3.4).¹³⁶ On the other hand, invoking the cooperation duties under Article 88quater CCP always requires the intervention of an investigating judge.

First, the investigating judge can order anyone to provide information on the operation and accessibility of the IT system or on the way to get access to the content in an understandable format.¹³⁷ It was not entirely clear whether a suspect could be obliged to provide information (e.g. a password) under this cooperation duty. In 2020, the Belgian Constitutional Court and the Court of Cassation decided that a suspect can indeed be ordered to provide a password under this provision and that such cooperation is not problematic in light of the right not to incriminate oneself.¹³⁸ Both domestic courts consider passwords to be material existing independent of the suspect's will (at the moment the cooperation is asked).¹³⁹ According to the Court of Cassation, it is required that the police discovered the IT system without coercion of the suspect, that it is

¹³¹ Kerkhofs and Van Linthout, *Cybercrime* 3.0, 333 and 422.

¹³² Art. 88bis(1), para. 5 CCP. An oral order with subsequent written confirmation is possible in urgent situations.

¹³³ Art. 88bis(2–3) CCP (Art. 27 2022 Data Retention Act).

¹³⁴ Art. 39bis(1–3) CCP (overt search IT system); Art. 88ter CCP (network search).

¹³⁵ Art. 39bis(4) CCP.

¹³⁶ Art. 90ter(1) CCP.

¹³⁷ Art. 88quater(1) CCP.

¹³⁸ Cour de cassation, 4 February 2020, No. P.19.1086.N, ECLI:BE:CASS:2020:ARR.20200204.2N.6; Cour de cassation, 19 December 2023, No. P.23.1157.N, ECLI:BE:CASS:2023:ARR.20231219.2N.2; Cour constitutionnelle, 20 February 2020, No. 28/2020.

¹³⁹ According to the European Court of Human Rights (ECtHR), the right not to incriminate oneself does not extend to material which has an existence independent of the will of the suspect, such as documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing (*Saunders/United Kingdom*, Appl. No. 19187/91, 17 December 1996, para. 69 and *Jalloh/Germany*, Appl. No. 54810/00, 11 July 2006, para. 102; see also Art. 7(3) and consideration 29 Directive: Directive 2016/343/EU of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in

established without reasonable doubt that the suspect knows the password and that the information asked is proportional with the investigation of the facts of the case.

Second, the investigating judge can order operation of the IT system or search of the data, making the data accessible, copying or deleting the data or blocking access thereto.¹⁴⁰ It was clarified in Parliament that the investigating judge can resort to this form of mandatory cooperation only when it is required, for instance when the IT system is too complex or when no qualified police personnel is present.¹⁴¹ The obligation is not absolute; legislation limits the duty of the cooperating party to what is ‘within their abilities’. The law explicitly states that this order cannot be given to the suspect or their relatives.

The persons subject to these cooperation duties have to be determined on a case-by-case basis, but the legislator gave some examples: importers/distributors of computers or software, so called trusted third parties, service providers, network operators, engineers responsible for the configuration of certain computer systems and security experts.¹⁴² These provisions provide a counterweight for the freedom to encrypt data under Article 107/5 ECA. Indeed, service providers can be ordered to decrypt data or to inform LEAs on how to decrypt it under Article 88quater CCP. The state is liable for all damage that the cooperating parties involuntarily cause to an IT system or the data.¹⁴³ It is up to the prosecuting authorities to prove that a person ‘can be deemed fit’ or ‘has special knowledge’.¹⁴⁴ If this is established in a convincing manner and is not plausibly countered by the service provider, non-cooperation is punishable.¹⁴⁵

Even if service providers refuse to cooperate with an overt search, the public prosecutor or investigating judge can still order (a) the temporary overriding of the security of the IT system concerned, if necessary using technical means, fake signals, fake keys (e.g. fingerprints) or fake identities; (b) the placing of technical means in the IT system concerned to decrypt or decode the data stored, processed or transmitted.¹⁴⁶ Hacking by LEAs is thus a legal possibility to get access to content data if the conditions for an overt search of an IT system or network search are fulfilled. The investigating judge or public prosecutor (depending on the scope of the search) can order this at all times, without the permission of the owner, rights holder or user. Contrary to when cooperation is sought, it is not provided that the state will be liable for any damage caused to an IT system or the data. Data obtained in such a manner can be used as evidence in court, with the same reservations as set out earlier (Section 9.1.2.2). Because data can be easily manipulated, it is essential that judges exercise great caution when assessing this evidence. Transparency about the hacking techniques and software used is crucial for this assessment. A similar possibility of hacking by LEAs exists in the context of the covert search of an IT system (see Section 9.3.3.4).

criminal proceedings, [2016] OJ L65/1, 11 March 2013). The ECtHR has yet to rule on the question of whether passwords constitute such material or even whether this criterion is adequate in this regard.

¹⁴⁰ Art. 88quater(2) CCP.

¹⁴¹ Explanatory Memorandum, *Doc. Parl.*, Ch. repr., sess. ord. 1999–2000, No. 50-0213/001, p. 27.

¹⁴² Explanatory Memorandum, *Doc. Parl.*, Ch. repr., sess. ord. 1999–2000, No. 50-0213/001, p. 27.

¹⁴³ Art. 88quater(5) CCP.

¹⁴⁴ Report on behalf of the Commission of Justice, *Projet de loi relative à la criminalité informatique*, *Doc. Parl.*, Sén., sess. ord. 1999–2000, No. 2-392/3, p. 69.

¹⁴⁵ Kerkhofs and Van Linthout, *Cybercrime* 3.0, 540.

¹⁴⁶ Art. 39bis(5) CCP. See also L. Urban and F. Verbruggen, ‘Pro-hacktive Policing: Covert Police Access to IT-Systems and Darknet Storefront’, in P. Valcke (ed.), *Technologie en recht* (Antwerpen: Intersentia, 2019), 21–48.

9.3.3.4 Interception of Data and Covert Search of an IT System

Article 90quater(2) and (4) CCP lists two cooperation duties for the investigative measure under Article 90ter CCP. Article 90ter deals with covert interception, taking knowledge of, searching and recording, with technical means, of the (1) private communication or (2) data of an IT system. It thus covers covert (live) interception of data and covert search of (the content of) an IT system.¹⁴⁷ This measure can be ordered by the investigating judge only in the context of a judicial inquiry (not through a mini-instruction).¹⁴⁸ It can target a suspect of one of the offences under Article 90ter(2–4) CCP, but also persons believed to frequently communicate with said suspect. The duration cannot be longer than one month, unless renewed (monthly renewals are possible until the sixth month).¹⁴⁹ If recordings (or copies) are made, appropriate measures must be taken to guarantee the integrity and confidentiality of the communication or data.¹⁵⁰ Some extra guarantees are provided for situations which might endanger legal or medical privilege as well.

Service providers' cooperation can be ordered under Article 90quater(2) CCP. Again, a Coordination Cell Justice, established by the service provider, will be tasked with compliance therewith.¹⁵¹ All communication intercepted should be communicated without delay to the National Technical and Tactical Support Unit (NTSU) of the federal police.¹⁵² Kerkhofs and Van Linthout complain about the reluctance of service providers to cooperate in practice, despite the severe penalty.¹⁵³ Another cooperation duty can be found in Article 90quater(4) CCP. This provision overlaps with the cooperation duties under Article 88quater CCP, but applies only to the specific measure of Article 90ter CCP.¹⁵⁴ Allowing the seeking of help from experts in decrypting the data sought, the latter cooperation duty can prove invaluable to Belgian LEAs.¹⁵⁵ Service providers falling under this provision can thus be forced to change the security settings to make interception possible.

If service providers refuse to cooperate under one of those provisions, if it is feared that they might not respect their secrecy obligations or when they are actually the target of a criminal investigation, the investigating judge can still order (a) the breaking into of a house, a private place or an IT system; (b) the temporary overriding of the security of the IT system, if necessary using technical means, fake signals, fake keys or fake identities; (c) the placing of technical means in the IT system concerned to decrypt or decode the data stored, processed or transmitted.¹⁵⁶ Hacking by LEAs is here thus also a legal possibility to get access to content data if the conditions to apply Article 90ter CCP are fulfilled. The investigating judge can order this at all times, without informing the owner, rights holder or user and without their consent. Data obtained in such a manner can be used as evidence in court, with the same reservations as set out earlier (Section 9.1.2.2).

¹⁴⁷ A similar provision (Art. 464/26 CCP) exists in the specific context of a criminal investigation regarding the execution of sentences.

¹⁴⁸ An oral authorisation with subsequent written confirmation is possible in urgent situations. Exceptionally, the prosecutor can order this measure (Art. 90ter(5) CCP).

¹⁴⁹ Arts. 90quater(1) and 90quinquies CCP.

¹⁵⁰ Art. 90septies(1) CCP.

¹⁵¹ Art. 2 modalities of cooperation RD.

¹⁵² Art. 5 modalities of cooperation RD.

¹⁵³ Kerkhofs and Van Linthout, *Cybercrime* 3.0, 466.

¹⁵⁴ Conings and Royer, 'Verzamelen digitaal bewijs in strafzaken', 325.

¹⁵⁵ Ibid.

¹⁵⁶ Art. 90ter(1), para. 3 CCP. See also Urban and Verbruggen, 'Pro-hacktive Policing', 21–48.

A special case in this regard is the hacking of crypto communication tools which are mainly – or arguably exclusively – used by criminals, such as EncroChat or Sky ECC. In 2021, in the course of a Belgian criminal investigation against cryptophone provider Sky ECC, LEAs intercepted, seized and decrypted millions of messages.¹⁵⁷ This provided useful information not only for the investigation against Sky ECC but also for other ongoing investigations and for the opening of new ones. Such a bulk data interception and seizure of course gives rise to questions, in particular concerning its proportionality and the criteria used to select data for further exploitation. Indeed, a judicial review concerning the proportionality of the measure and the possibility for the defence to effectively comment on the selection of data will be crucial in these cases.¹⁵⁸ Under Belgian criminal procedure rules, LEAs can keep the technical means and police methods that have been used for covert surveillance secret (e.g. Articles 47sexies-septies CCP). Somewhat confusingly, Article 47sexies(1), para. 3 CCP explicitly excludes ‘technical means’ within the meaning of Article 90ter CCP. Article 47sexies(1) predates the 2016 Internet Investigatory Powers Act that legalised ‘hacking by LEAs’ when updating Articles 39bis and 90ter ff. CCP, which makes one wonder what the legislative intent was. Insofar as software inevitably has the potential to alter data, it remains to be seen to what extent defendants and trial judges will be informed about the hacking techniques used, when the authenticity of the data is challenged. The Belgian Court of Cassation has always shown great understanding for the difficulties encountered by LEAs, so it seems likely that it will not push for transparency as to the hacking techniques or software used and that it will focus instead on the evidence that has been obtained.

9.3.3.5 Blocking of Access to Data or Websites

Service providers’ cooperation can also be necessary to block access to data (often a website). When LEAs are confronted with websites that are used to commit criminal offences, seizure of the data carrier is often not satisfactory. Deleting or making data inaccessible is then desirable. Article 39bis(6), para. 3 CCP allows the public prosecutor to harness the appropriate technical means to prevent access to the data in the IT system and the copies thereof and to secure the integrity of the data. The Court of Cassation clarified that an order to block the website addressed to an IAP can be considered ‘appropriate technical means’ under this provision.¹⁵⁹

The scope of this cooperation duty is not necessarily limited to IAPs; the Court of Cassation refers to IAPs as an example of ‘others than those storing the data themselves or those letting a third party store the data’.¹⁶⁰ The fact that the Court has read a cooperation duty under this provision

¹⁵⁷ Press release ‘Des messages décryptés donnent un aperçu unique du fonctionnement des organisations criminelles’, 10 March 2021, www.police.be/5998/fr/actualites/des-messages-decryptes-donnent-un-apercu-unique-du-fonctionnement-des-organisations; press release ‘09/03/2021 – 09/03/2022: SKY 1 an d’enquête’, 10 March 2022, www.police.be/5998/fr/presse/09032021-09032022-sky-1-an-denquete.

¹⁵⁸ From the first Belgian judgments it can be concluded that adding documents from the criminal file of the investigation against Sky ECC that allow assessing how other suspects were identified is (rightfully) considered essential. The Court of Cassation also already stressed that the defence has no unqualified right to the inclusion of all data it deems necessary to ascertain that the other criminal file is not tainted by irregularities (Cour de cassation, 31 October 2023, No. P.23.0998.N, ECLI:BE:CASS:2023:ARR.20231031.2N.2).

¹⁵⁹ Cour de cassation, 22 October 2013, No. P.13.0550.N, ECLI:BE:CASS:2013:ARR.20131022.4. In our view, this has not been codified by the 2016 Internet Investigatory Powers Act. However, since 2020 the legislator seems to read this cooperation duty into Art. 39bis(6), para. 6 CCP. Indeed, the then introduced misdemeanour of refusing to cooperate refers to Art. 39bis(6), para. 6 CCP (Art. 7 Loi visant à combattre la diffusion non consensuelle d’images et d’enregistrements à caractère sexuel (Non-consensual Dissemination of Sexual Content Act), 4 May 2020, MB 18 May 2020, current Art. 417/56 CC).

¹⁶⁰ Cour de cassation, 22 October 2013.

without much support in the text or preparatory documents has been rightly criticised.¹⁶¹ The idea that, in the context of the seizure of data (usually ordered against a suspect), an order can be issued against a third party who is merely the provider of access to the data is indeed rather odd. Especially since this does not prevent the actual administrators from accessing and manipulating their illegal website and data. The execution of such an order does not guarantee in any way the integrity of the data, which is one of the objectives of the seizure of data.¹⁶² Furthermore, it is not legally defined how long the blocking of the website should last, which creates legal uncertainty (for instance when the public prosecutor refrains from further prosecution).¹⁶³ The Court of Cassation also did not provide clarity on this matter. Although Articles 19 and 25 of the Belgian Constitution crystallise a liberal nineteenth-century approach to free speech and explicitly ban any form of censorship, the Constitutional Court itself has not yet pronounced on the matter.

Websites having the ‘.eu’ or the ‘.be’ domain name fall under the responsibility of two companies (EURid and DNS.be) headquartered in Belgium. An order to make the website inaccessible (by revoking the domain name) addressed to these companies consequently does not give rise to any jurisdiction problems. Since this means that all pages of the website become inaccessible, Kerkhofs and Van Linthout state that it should not be used when there is also legal content on the website or when the criminal character of the offence is not with a large majority agreed upon by other countries.¹⁶⁴ For domain names registered in a foreign country, an order to Belgian IAPs (Telenet, Proximus ...) to block the domain name system (DNS) is indeed a possibility.¹⁶⁵ However, the website would then become non-accessible only for Belgian customers of the IAP and blocking of a DNS can also be easily circumvented.¹⁶⁶ A more adequate solution is an order to Belgian IAPs (on the same legal basis) to block a website by way of a recurring reverse IP domain check (‘searching of all different domain names that refer to the same IP-address (which forms the object of the seizure’)).¹⁶⁷ As of 7 June 2022, hosting service providers offering services in the EU that disseminate information to the public can also be ordered to remove or disable access to online terrorist content on the basis of Regulation 2021/784.¹⁶⁸

9.3.3.6 Expedited Preservation of Data

Another form of mandatory cooperation relates to the expedited preservation of data.¹⁶⁹ The data then has to be preserved by the addressee of the cooperation duty, but will not yet be delivered to LEAs and does not yet become accessible by them.¹⁷⁰ Mostly, this order precedes another investigative measure such as an order to disclose the data or seizure. It is particularly useful when it is likely that data will be deleted shortly or to remedy, to a certain degree, the lack of a general data retention obligation.

¹⁶¹ P. Monville and M. Giacometti, ‘Les fournisseurs d’accès à internet, nouveaux gendarmes de la toile’ (2014) 2 *Revue du droit des technologies de l’information* 74; Conings and Royer, ‘Verzamelen digitaal bewijs in strafzaken’, 331.

¹⁶² R. Schoefs, ‘Strijd tegen the Pirate Bay over andere boeg gegooit: databeslag toegestaan’ (2014) 2 *Tijdschrift voor Strafrecht* 131–142; Conings and Royer, ‘Verzamelen digitaal bewijs in strafzaken’, 331.

¹⁶³ Conings and Royer, ‘Verzamelen digitaal bewijs in strafzaken’, 331.

¹⁶⁴ Kerkhofs and Van Linthout, *Cybercrime* 3.0, 225–226.

¹⁶⁵ Ibid., 226.

¹⁶⁶ Ibid., 227–228.

¹⁶⁷ Ibid., 228–229.

¹⁶⁸ Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, [2021] OJ L172/79, 17 May 2021.

¹⁶⁹ An oral order with subsequent written confirmation is possible in urgent situations.

¹⁷⁰ Conings and Royer, ‘Verzamelen digitaal bewijs in strafzaken’, 326.

Article 39ter CCP encompasses domestic situations and constitutes the Belgian implementation of Articles 16–17 of the Cybercrime Convention. First, as it applies to ‘data stored, processed or transmitted by means of an IT system’, the Belgian provision is broader than what the Cybercrime Convention dictates.¹⁷¹ Second, it is not only traffic data that can be preserved under the Belgian preservation; any type of data (including content data) that is particularly vulnerable to loss or modification is covered.¹⁷²

The cooperation duty under Article 39ter CCP is addressed to one or several individuals or legal persons who have the data in their possession or under their control. The Explanatory Memorandum refers only to bona fide possession or control,¹⁷³ but this (obvious) clarification has not been inserted into Article 39ter CCP. Mostly, that person will be an operator or provider of an electronic communications service. Expedited preservation lasts in principle a maximum of ninety days, but an indefinite number of renewals is possible.¹⁷⁴ The lawmakers have failed to indicate situations in which preservation would entail making data non-accessible (freezing of data).¹⁷⁵

9.3.3.7 Future Preservation of Data

The 2022 Data Retention Act inserted a new cooperation duty into the CCP (Article 39quinquies). The government, who had taken the initiative for the legislation, thought that an order to retain traffic and location data in the context of a criminal investigation which targets a certain person or group of persons could be a measure that is compatible with the case law of the CJEU.¹⁷⁶ The data has to be retained after an order by the public prosecutor, but law enforcement may not obtain access immediately. Such access will be granted only after the separate procedure of Article 88bis CCP.¹⁷⁷ The public prosecutor in a written order has to explicitly state the duration of the measure (a maximum of two months, with the possibility of renewal) and the duration of the retention (a maximum of six months, with the possibility of renewal).¹⁷⁸ One or more of the following elements should also be indicated with precision: the person(s) concerned, the means of communication targeted and the places for which retention is required. It remains to be seen to what extent this new provision will be applied by LEAs in practice.

9.3.4 *Legal Remedies and Protection of Fundamental Rights*

9.3.4.1 Notification and Information

No general provision requires that individuals should be notified of the fact that their data has been accessed or delivered to LEAs following the cooperation of a service provider in the context

¹⁷¹ Art. 16(1) Cybercrime Convention refers to ‘the expeditious preservation of specified computer data, including traffic data, *that has been stored by means of a computer system*’ (emphasis added).

¹⁷² Franssen, ‘The Belgian Internet Investigatory Powers Act’, 537.

¹⁷³ Explanatory Memorandum, *Doc. Parl.*, Ch. repr., sess. ord. 2015–2016, No. 54-1966/001, p. 26.

¹⁷⁴ Monville, Giacometti and Grisard, ‘Collecte des preuves numériques après l’arrêt du 5 décembre 2018’, 1003.

¹⁷⁵ Conings and Royer, ‘Verzamelen digitaal bewijs in strafzaken’, 327 (the Cybercrime Convention leaves this to the national level).

¹⁷⁶ Explanatory Memorandum, *Doc. Parl.*, Ch. repr., sess. ord. 2021–2022, No. 55-2572/001, p. 9; See *La Quadrature du Net*, §§147–149.

¹⁷⁷ Art. 39quinquies(4) CCP.

¹⁷⁸ Art. 39quinquies(1), para. 3 CCP. An oral order with subsequent written confirmation is possible in urgent situations.

of a criminal investigation. The Belgian implementation of the Law Enforcement Directive¹⁷⁹ by the Act of 30 July 2018¹⁸⁰ does not regulate this either. The person whose personal data is being processed has a right to be informed and a right to request access under this Act.¹⁸¹ However, it is further added that the law can limit those rights, insofar and as long as the limitation is necessary and proportionate, to (1) prevent any obstruction of criminal or other investigations or procedures; (2) avoid detrimental consequences for the prevention, detection, investigation and prosecution of punishable offences or execution of punishments; (3) protect public security; (4) protect national security; and (5) safeguard the rights and freedoms of others.¹⁸² A data subject requesting access¹⁸³ will in principle, without unnecessary delay, be notified in writing of the refusal or limitation of access.¹⁸⁴ Furthermore, they will also be informed of the possibility of judicial review or a complaint to the supervisory authority.¹⁸⁵ Regarding the exercise of these rights when personal data has been incorporated in a judicial file or is being processed in the context of a criminal investigation or procedure, it is even explicitly stated that the procedure under the CCP has to be followed.¹⁸⁶

So, there is no general right to information or access.¹⁸⁷ In principle, a criminal investigation is secret. Any cooperating person or entity and anyone who, by virtue of their office, is informed of investigative measures often has to keep the cooperation secret as well. This confidentiality obligation is applicable to all cooperation duties set out earlier (see Section 9.3.3) with the sole exception of the blocking of access to data or websites. Any breach of the confidentiality duty will be punishable as violation of professional secrecy with imprisonment of one to three years and/or a fine of 800 to 8,000 euros for natural persons and 48,000 to 576,000 euros for legal persons.¹⁸⁸

Quite problematic is that the law has not determined the duration of this duty of confidentiality. This makes it difficult for any cooperating service provider to estimate when they can inform the data subject involved. As regards the expedited preservation of data, this is even despite Article 16(3) of the Cybercrime Convention clearly indicating that the duty of confidentiality will last ‘for the period of time provided for by its domestic law’.¹⁸⁹ When cooperation is ordered under Article 88quater CCP in the context of an overt search, the person responsible for the IT system has to be notified of the search as soon as possible and has to receive a summary of the data copied, made inaccessible or deleted.¹⁹⁰ The Constitutional Court has interpreted this duty as also covering the data subject (whether or

¹⁷⁹ Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, [2016] OJ L119/89, 4 May 2016.

¹⁸⁰ Loi relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel (Personal Data Processing Act (PDPA)), 30 July 2018, MB 5 September 2018. On the Belgian implementation, see also C. Forget, ‘Protection des données dans le secteur de la “police” et de la “justice”’, in V. Franssen and D. Flore (eds.), *Société numérique et droit pénal. Belgique, France, Europe* (Brussels: Bruylant, 2019), 327–366, especially 349–354.

¹⁸¹ Arts. 37(1) and 38(1) PDPA.

¹⁸² Arts. 37(2) and 38(2) PDPA.

¹⁸³ Which already presupposes that the data subject knows their data is being processed by LEAs.

¹⁸⁴ Art. 38(3) PDPA.

¹⁸⁵ Ibid.

¹⁸⁶ Art. 44 PDPA.

¹⁸⁷ Art. 11 of Regulation 2021/784 does contain a regime for the making available of information to content providers (users) on the removal or disabling of terrorist content.

¹⁸⁸ Art. 458 CC.

¹⁸⁹ Franssen, ‘The Belgian Internet Investigatory Powers Act’, 537.

¹⁹⁰ Art. 39bis(7) CCP (unless that person’s identity or residence cannot be reasonably found).

not that person is a suspect), even when that person is not the person responsible for the IT system.¹⁹¹ The duty of confidentiality would then no longer apply.

Regarding the covert data interception measure, a notification regime has been explicitly laid down in Article 90novies CCP. Parliament deemed this necessary when it first allowed wiretapping in the 1990s because it considered that this investigative measure implied a major invasion of a person's right to privacy.¹⁹² At the latest fifteen days after the decision by the investigation supervision court to refer the case to the Court of First Instance or the Court of Appeal has become final, the court clerk will notify any person (suspects and other data subjects) who has been the subject of a measure under Article 90ter CCP.¹⁹³ The written notification should contain the nature of the measure as well as the days when it was performed. A request by the public prosecutor is also required, but this cannot be seen as a *conditio sine qua non*. Even without the request, notification is mandatory, in our view. Only when the identity and/or the residence of that person cannot be reasonably found will there be no obligation to notify. The obligation of secrecy would, regarding the information mentioned under Article 90novies CCP, also end (at the latest) at that point in time.

The above notification does not necessarily seem to entail that a data subject or suspect is informed of the cooperation of a service provider. It certainly does not allow them to verify whether the applicable rules were respected. During the judicial inquiry and proceedings before a court, only the civil party, anyone against whom the criminal proceedings have been brought and their lawyers can request a copy of the recorded private communications or the not publicly available data of an IT system.¹⁹⁴ This is also an indispensable guarantee to allow them to verify the integrity of the data when hacking by LEAs took place. In case of bulk interception, it remains to be seen how other data subjects whose communications have also been caught will be protected. It seems that the 'exclusively criminal use' of cryptophone systems intercepted in operations like Encrochat or Sky ECC makes it less likely that the communication of innocent users was intercepted.

Under all other circumstances, the data subjects that are involved in criminal proceedings will probably notice that a service provider must have cooperated with LEAs at the time when they get access to the criminal file. In general, during the investigation, persons who have a direct interest (e.g. a suspect or civil party, certainly not every data subject) can request access to and a copy of the criminal file.¹⁹⁵ A request of access can be denied by the public prosecutor, or the investigating judge (in the case of a judicial inquiry), when (1) this is required for the investigation; (2) access would create danger for persons or a serious violation of their privacy; (3) the party submitting the request does not demonstrate a rightful motive for access. Any other third party with a legitimate interest (e.g. a service provider or someone whose communication was also intercepted but is not involved in the criminal investigation) can request from the public prosecutor access to and a copy of the criminal file as well.¹⁹⁶ The public prosecutor can reject such a request without justification and without a remedy being available. For users of

¹⁹¹ Cour constitutionnelle, 6 December 2018, B.15.2 and B.22.2; W. Yperman, S. Royer and F. Verbruggen, 'Vissen op de grote datazee: Digitale informatievergaring in vooronderzoek en strafuitvoering' (2019) 5 *Nullum Crimen* 393, para. 10.

¹⁹² Explanatory Memorandum, Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, *Doc. Parl.*, Sén., sess. ord. 1992–1993, No. 843-1, p. 18.

¹⁹³ A similar notification exists in the context of a criminal investigation regarding the execution of sentences.

¹⁹⁴ Art. 90septies(6) CCP.

¹⁹⁵ Arts. 21bis and 61ter CCP.

¹⁹⁶ Art. 21bis(1), para. 3 CCP.

communication whose data might have been intercepted as ‘bycatch’, this right can, however, not really be considered effective: only rarely will they have knowledge of the investigative measure, to request and receive access.

At the end of a judicial inquiry, an investigation supervision court will have to determine whether the case will be referred to court. At least fifteen business days before that hearing, the civil party, persons who have the formal status of injured party and anyone against whom criminal proceedings have been brought (and their lawyers) will be informed that they now have access to the criminal file.¹⁹⁷ When the investigation has been conducted by a public prosecutor, the case can be immediately referred to court. In those situations, all parties involved in the criminal proceedings before the court will have a right to access the criminal file.¹⁹⁸

9.3.4.2 Judicial Review and Redress

There are no specific rules allowing for judicial review when the rules applicable to a cooperation duty have not been respected,¹⁹⁹ but the general rules of criminal procedure might result in judicial review. When the data has been seized, legislation provides for a procedure to request the lifting of a seizure.²⁰⁰ The Constitutional Court has indicated that this procedure was one of the guarantees compensating the fact that an officer of the judicial police can perform an overt search of an IT system.²⁰¹ Although certainly not created for that purpose, this would mean that an unlawful intrusion of one’s privacy can be remedied under this procedure.²⁰²

A second possibility for judicial review is an appeal to the indictments chamber (*chambre des mises en accusation*, an investigation supervision court) which is, for instance, possible when access to the criminal file has not been granted to any of the persons who have a direct interest.²⁰³ Said indictments chamber can then also rule on irregularities concerning previously executed investigative measures.²⁰⁴ This possibility is, however, limited to appeals to the indictments chamber during a judicial inquiry; it does not apply during the preliminary investigations conducted by the public prosecutor.²⁰⁵

At the end of a judicial inquiry the investigation supervision court can, before referring the case to court, assess the regularity of the investigative measures.²⁰⁶ If the investigation supervision court does not consider the investigative measures to be unlawful, the same arguments regarding regularity can later be presented again before the trial court.²⁰⁷ An appeal to the indictments chamber against the decision of the council chamber is possible as well. When the investigation has been finalised by a public prosecutor and the case is brought before a court, it will be for that court to verify the regularity of the investigative measures. Finally, a possibility of judicial redress

¹⁹⁷ Art. 127(2) CCP (the period is three days when anyone against whom criminal proceedings have been brought is detained); Verstraeten, ‘Handboek strafvordering’, 662–663, para. 1304.

¹⁹⁸ Verstraeten, ‘Handboek strafvordering’, 929–930, para. 1852.

¹⁹⁹ Art. 9 of Regulation 2021/784 on addressing the dissemination of terrorist content online does, however, provide a right to an effective remedy for both hosting service provider and content provider (user) following a removal order.

²⁰⁰ Arts. 28sexies and 61quater CCP. This thus includes the blocking of access to data or websites under Art. 39bis(6), para. 3 CCP.

²⁰¹ Cour constitutionnelle, 6 December 2018, B.8.5.

²⁰² Yperman, Royer and Verbruggen, ‘Digitale informatievergaring in vooronderzoek en strafuitvoering’, 394, para. 11.

²⁰³ Art. 61ter(5) CCP.

²⁰⁴ Art. 235bis CCP.

²⁰⁵ Cour de cassation, 20 April 2010, No. P.09.1750.N, ECLI:BE:CASS:2010:ARR.20100420.2.

²⁰⁶ Arts. 131 and 235bis CCP.

²⁰⁷ Verstraeten, ‘Handboek strafvordering’, 683, para. 1330.

is to bring a civil action for damages against the state on the basis of Article 1382 of the Belgian Civil Code if the unlawful cooperation caused harm.

9.3.4.3 Some Failings in the Current Legal Framework

Problems that were directly linked with cooperation duties have already been highlighted (Section 9.3.3). Other human rights issues concern the underlying investigative measures underpinning cooperation duties. We do not intend to provide an exhaustive list here, but we can point out some controversial issues.

First, the Internet Investigatory Powers Act wanted – rightly so – to end the differentiation between the (cooperation duties related to the) classic wiretapping of a telephone and the (live) interception of the data of an IT system. Both types of intervention were linked to the conditions and guarantees that used to be provided for old-school wiretapping. With this choice, lawmakers ignored that, when secretly intercepting and searching the data of an IT system, LEAs can get access to significantly more and more sensitive information (e.g. bank account information,²⁰⁸ emails, messages sent on dating apps or websites, pictures ...) than when overhearing classical telephone conversations.²⁰⁹ More procedural safeguards would thus, in our opinion, have been logical in the light of human rights protection. Belgium also failed to reconsider the historically understandable but technologically obsolete distinction between visual surveillance with the use of technical means ('covert observation') on the one hand and auditive surveillance ('wiretapping') on the other hand. The latter has, in view of the evolution of communication technology (communication apps, video messaging ...), been expanded while the former was not integrated and remains subject to different rules. From a privacy perspective, it does not seem to matter that much whether the police have placed the hidden camera itself (covert observation) or rather hacked someone else's camera (wiretapping): what matters is the type of information the LEAs get access to. That is more in general the problem with the (Belgian) legal framework: rather than on the amount and type of information, the regulation still excessively focuses on the way in which information has been gathered by LEAs.²¹⁰ Historically, that may have been an adequate criterion to determine the degree of intrusiveness, as live interception was the only way to get hold of private communication. Nowadays, the most personal and intimate communication often is still available and consultable afterwards. The European initiatives (see Section 9.4.4) focus more on the type of data, which makes more sense, but they do not yet seem to offer immediately usable criteria for national lawmakers regulating the gathering of e-evidence.

The Belgian choice not to require a judicial intervention for certain investigative measures, although blessed by the Constitutional Court,²¹¹ seems controversial as well, especially in light of the CJEU's 2020 and 2021 data retention judgments. This makes it, for instance, questionable that an overt search of an IT system and an order to produce identification data can be authorised by the public prosecutor²¹² (Sections 9.3.3.2 and 9.3.3.3)²¹³ and that the expedited preservation of

²⁰⁸ See Art. 46quater CCP.

²⁰⁹ Yperman, Royer and Verbruggen, 'Digitale informatievergaring in vooronderzoek en strafuitvoering', 411, para. 59.

²¹⁰ On this, see also Conings, 'Klassiek en digitaal speuren', 292–323.

²¹¹ Cour constitutionnelle, 6 December 2018, B.8.7 and B.9.5; Cour constitutionnelle, 18 November 2021, No. 158/2021, B.16.8.6.

²¹² It is a fortiori problematic that the officer of the judicial police is competent to order an overt search of an IT system.

²¹³ *Prokuratuur*, §§51–59. It is not entirely clear whether a (prior) review carried out either by a court or by an independent administrative body is required by the CJEU for access to identification data. According to the Constitutional Court it is not (Cour constitutionnelle, 18 November 2021, B.16.8.6), but we and others (P. Tersago, 'EHRM aanvaardt retentie en toegang tot identificatiegegevens van prepaid telefoonkaarten' (2020) 2

data can be ordered by an officer of the judicial police (Section 9.3.3.6),²¹⁴ all three without judicial intervention.

The Constitutional Court²¹⁵ did insist on special thresholds to protect legal and medical privilege if the IT systems of privileged persons are searched, but it remains doubtful whether the regime complies with the standards of the European Court of Human Rights (ECtHR).²¹⁶ It is not the representatives of the legal or medical professional organisations but, rather, the investigating authorities that decide on whether information is privileged and whether it can be used. Belgian law also does not contain any protection for privileged information that is stored not by a professional but by the client or patient.

Also very questionable is the fact that there are barely any sanctions when rules are violated. This can be partly explained by the existence of Article 32 PT CCP, which provides only a limited list of situations when evidence can be excluded (Section 9.1.2.2). A more active role for the judge, allowing for special attention to be paid to proportionality and subsidiarity and whereby the exclusion of illegally gathered evidence is more than an exceptional sanction, would be our recommendation,²¹⁷ if only to meet the requirements of Article 13 of the ECHR concerning the right to an effective remedy, for instance when the right to privacy has been violated.²¹⁸

9.4 CROSS-BORDER COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

9.4.1 Introduction

To determine whether a situation is cross-border, we refer to the criteria mentioned earlier (Section 9.3.1.2). In cross-border situations, there is a mixture of mandatory and voluntary cooperation, but in a Belgian context a clear-cut distinction between the two is hard to make.

Owing to the broad territorial scope of Articles 46bis, 88bis and 90quater(2) CCP, unilateral and mandatory direct cooperation with foreign service providers is deemed possible (Section 9.3.1.2.2). This unilateral approach creates some issues. First, even though it can be argued that many states implicitly consent to the practice, authors like Tosza stress that such an approach remains questionable in light of international law and especially the principle of sovereignty.²¹⁹ Second, if Belgian LEAs can force any foreign service provider offering services in Belgium to cooperate, Belgium has less authority to complain about other countries that have even less procedural safeguards doing the same.²²⁰ Third, even if domestic LEAs can order service providers to cooperate, they still need jurisdiction to enforce this duty to make it a ‘real obligation’. Yahoo!, for instance, did not have any

Tijdschrift Privacy & Persoonsgegevens 30) are inclined to disagree and think that the CJEU considers this a general requirement for access to retained data. A question to the CJEU to settle the matter would be welcome.

²¹⁴ *La Quadrature du Net*, §163.

²¹⁵ Cour constitutionnelle, 6 December 2018, B.24.1–B.27. See also Cour constitutionnelle, 29 April 2021, No. 66/2021.

²¹⁶ See, e.g., *Golovan/Ukraine*, Appl. No. 41716/06, 5 July 2012; *Servulo & Associados – Sociedade de Advogados, RL and others/Portugal*, Appl. No. 27013/10, 3 September 2015; *Lindstrand Partners Advokatbyrå AB/Sweden*, Appl. No. 18700/09, 20 December 2016; *Leotsakos/Greece*, Appl. No. 30958/13, 4 October 2018; *Kirdök and others/Turkey*, Appl. No. 14704/12, 3 December 2019; *Saber/Norway*, Appl. No. 45918, 17 December 2020.

²¹⁷ Yperman, Royer and Verbruggen, ‘Digitale informatievergaring in vooronderzoek en strafuitvoering’, 415, para. 68; Verbruggen and Conings, ‘Return to Reasonable Rules on Illegally Obtained Evidence?’, 305.

²¹⁸ Yperman, Royer and Verbruggen, ‘Digitale informatievergaring in vooronderzoek en strafuitvoering’, 415, para. 69.

²¹⁹ S. Tosza, ‘Cross-Border Gathering of Electronic Evidence: Mutual Legal Assistance, Its Shortcomings and Remedies’, in V. Franssen and D. Flore (eds.), *Société numérique et droit pénal: Belgique, France, Europe* (Brussels: Bruylant, 2019), 276.

²²⁰ De Schepper, ‘Cassatie bevestigt rechtstreeks gegevens vorderen van Yahoo’, 492; Verbruggen and De Schepper, ‘Ontsnappen space invaders aan onze pacmannen?’, 162; Verbruggen and Royer, ‘Veroordeling Skype niet verbroken’, 1442.

assets on Belgian soil, which would have made it hard to execute any conviction to pay a fine after cooperation was refused.²²¹ Fourth, if every country were to adopt a similar approach, this would result in a complex multiplicity of different connecting factors and thus an increase of legal uncertainty for service providers and data subjects.²²² Last, more privacy-sensitive countries could react with laws prohibiting service providers from cooperating with foreign LEAs, creating more legal conflicts and undermining truly voluntary cooperation.²²³ The Belgian government appears to realise that the current solution is a short-term one, hence its intention to engage in working on more sustainable solutions on a supranational level.

Apart from the notification under Article 88ter, para. 4 CCP (Section 9.3.1.2.2), no particular rules exist to respect the sovereignty of other states. Belgian law also does not contain any data localisation requirements.

9.4.2 Cooperation of National LEAs with Foreign Service Providers

9.4.2.1 Legal Framework

9.4.2.1.1 CYBERCRIME CONVENTION. Belgium signed the Cybercrime Convention on 23 November 2001, but only ratified it on 20 August 2012.²²⁴ Ratification took more than ten years because initially lawmakers intended to ratify the Convention and its First Additional Protocol simultaneously.²²⁵ However, bringing Belgian legislation in line with Article 6 of the First Additional Protocol proved to be politically difficult. The government eventually decided to split up the ratification of both instruments.²²⁶ Only in 2019, anti-discrimination legislation was changed in accordance with the First Additional Protocol.²²⁷ Belgium should therefore be able to ratify the First Additional Protocol in the near future. Meanwhile, a Second Additional Protocol to the Convention has been adopted providing, inter alia, a legal basis for direct cooperation with foreign service providers for subscriber information and enhanced cooperation tools for the disclosure of subscriber information and traffic data.²²⁸ Belgium was one of the first states to sign this Protocol on 12 May 2022, but has yet to ratify it.²²⁹

Prior to ratification, the domestic legal framework was already fairly in line with the Cybercrime Convention.²³⁰ The Internet Investigatory Powers Act transposed Articles 16, 17,

²²¹ De Schepper, 'Cassatie bevestigt rechtstreeks gegevens vorderen van Yahoo', 493.

²²² Franssen, 'The Belgian Internet Investigatory Powers Act', 540. See also European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, COM/2018/225 final – 2018/0108 (COD), 17 April 2018, 1.

²²³ Verbruggen, 'Zesde rechter in Belgische Yahoozaak schaaft zich achter eerste', 9.

²²⁴ 'Chart of Signatures and Ratifications of Treaty 185', www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185.

²²⁵ Council of Europe, *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems*, ETS No. 189, 28 January 2003.

²²⁶ Report on behalf of the Commission of Foreign Affairs and National Defence, *Projet de loi portant assentiment à la Convention sur la cybercriminalité*, faite à Budapest le 23 novembre 2001, *Doc. Parl., Sén., sess. ord. 2011–2012*, No. 5-1497/2, p. 5.

²²⁷ Art. 115 *Loi portant des dispositions diverses en matière pénale et en matière de cultes, et modifiant la loi du 28 mai 2002 relative à l'euthanasie et le Code pénal social*, 5 May 2019, *MB* 24 May 2019.

²²⁸ Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence*, No. 224, 17 November 2021.

²²⁹ 'Chart of Signatures and Ratifications of Treaty 224', www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224.

²³⁰ Explanatory Memorandum, *Projet de loi portant assentiment à la Convention sur la cybercriminalité*, faite à Budapest le 23 novembre 2001, *Doc. Parl., Sén., sess. ord. 2011–2012*, No. 5-1497/1, pp. 2–28. See also the legislative profile of Belgium, www.coe.int/en/web/octopus/country-wiki.

29 and 30 of the Convention and introduced expedited preservation under Articles 39ter-quater CCP.²³¹ The domestic legal framework nevertheless diverges from the Convention in some respects (see also Sections 9.3.1.2.2 and 9.3.3.6). Belgium failed to implement Article 17(1)(b) of the Cybercrime Convention under Article 39ter CCP, but this might be covered under the cooperation duties of Articles 46bis and 88bis CCP.²³²

If the data to be preserved is located in the territory of another state, in principle Article 39quater(1) CCP applies. The request under this provision aims to guarantee that data will still be available when a legal assistance procedure is initiated later. Under Article 39quater(1) CCP, the Belgian public prosecutor or investigating judge has to request the foreign competent authority, through the FCCU, to order the expedited preservation of data. The material scope of Article 39quater(1) CCP corresponds with the scope of Article 39ter CCP, which we referred to in Section 9.3.3.6. Although possible under Article 39quater(1), a Belgian request concerning non-stored data is likely to be rejected by the foreign state.²³³ As the procedure of Article 39quater(1) does not necessarily have to be followed in cross-border situations (Section 9.3.1.2.2), applications of this provision will probably be rare.²³⁴

9.4.2.1.2 EUROPEAN INVESTIGATION ORDER (EIO) DIRECTIVE. As one of the member states behind the initial proposal that led to the 2014 EIO Directive,²³⁵ Belgium implemented it by the Act of 22 May 2017.²³⁶ Although the EIO is a positive evolution for the collection of classic offline evidence, it is not the most appropriate means to gather cross-border e-evidence. Deadlines under the EIO Directive are considered too long, which is especially problematic for digital evidence where time is of the essence. The EIO Directive also does not include any sanctions if these time limits are not met. In the case of a systematic breach of deadlines, the Commission can, however, start an infringement procedure.²³⁷

The EIO is useful only when the state where the evidence can be located is easily identifiable.²³⁸ For digital evidence, this is rarely an exercise with a straightforward answer. Solely in the situation where digital evidence can be located in a certain state, when receipt of the data carrier is desirable and when there is no risk of deletion or modification of data will the EIO prove its worth.²³⁹ Since alternatives do exist, that is, voluntary cooperation (Section 9.4.2.2) and mandatory cooperation for service providers offering targeted services within Belgian territory (Sections 9.3.1.2.2 and 9.4.1), the situations in which Belgian LEAs will resort to the heavy and lengthy EIO procedure will in practice be limited.²⁴⁰

9.4.2.1.3 MUTUAL LEGAL ASSISTANCE TREATIES (MLATS). The well-known shortcomings of MLATs have been raised in a national context; we will discuss the Belgium–USA MLAT to

²³¹ Explanatory Memorandum, *Doc. Parl.*, Ch. repr., sess. ord. 2015–2016, No. 54-1966/001, pp. 9 and 25–26.

²³² Franssen and Leroux, ‘Recherche policière et judiciaire sur internet’, 173.

²³³ *Ibid.*, 174.

²³⁴ *Ibid.*

²³⁵ Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, [2014] OJ L130/1, 1 May 2014.

²³⁶ Loi relative à la décision d’enquête européenne en matière pénale (European Investigation Order Act), 22 May 2017, MB 23 May 2017.

²³⁷ D. Van Daele, ‘België en het Europees onderzoeksbevel in strafzaken: Een analyse van de wet van 22 mei 2017’ (2018) 4 *Nullum Crimen* 360.

²³⁸ Giacometti, ‘Décision d’enquête européenne, moyen approprié?’, 316 and 324.

²³⁹ *Ibid.*, 324.

²⁴⁰ *Ibid.*, 316 and 324.

illustrate them.²⁴¹ Since the USA–EU MLAT does not provide a legal basis on which to request digital evidence,²⁴² the 1988 Belgium–USA Treaty²⁴³ comes into play. The legal assistance under this Treaty concerns, inter alia, localisation or identification of persons and communication of data.²⁴⁴ Under Article 6 of this Treaty, production orders (for data) can be issued.

An MLA request has to be sent to the Belgian Minister of Justice, or their representative or delegate, who then subsequently sends it to the US Attorney General, or their representative.²⁴⁵ The request has to be processed as soon as possible, but according to the procedures of the requested state.²⁴⁶ Consequently, authorisation by a US court is needed, which also means that the requirement of probable cause (that the requested data is evidence of a punishable offence) has to be met.²⁴⁷

On average, MLA requests to the USA take ten months to fulfil and sometimes even considerably longer.²⁴⁸ Such a long delay is a particular hurdle when confronted with the volatility of digital evidence and the fast pace of operations regarding it.²⁴⁹ Requests are also often not carried out at all and just sent back to the Belgian authorities.²⁵⁰ This might have something to do with the requirement of probable cause, which often seems too high of a burden for Belgian LEAs, especially in the early stages of a criminal investigation. Since this is a non-familiar concept, European LEAs indeed often struggle to meet this condition.²⁵¹ Other flaws of the MLAT procedure are its complexity, its cost and, consequently, the disproportionality of the procedure if applied to purely domestic cases.²⁵² These flaws sometimes result in incorrect or inadequate requests as well.²⁵³

Unilateral direct cooperation with foreign service providers is considered a solution to overcome these shortcomings. Moreover, the Belgian authorities have entered into understandings with major US-based service providers for direct requests regarding non-content data (Section 9.4.2.2). Finally, if Belgium has no MLAT with a third country and has no powers under the Cybercrime Convention or the EIO Directive, national LEAs can also try to get data from that country through diplomatic means.²⁵⁴

²⁴¹ These are mostly, with the exception of the ‘probable cause’ requirement, also relevant for other MLATs Belgium has closed (for instance with Brazil, Canada, China, India and Korea).

²⁴² Tosza, ‘Gathering Electronic Evidence: Mutual Legal Assistance’, 271.

²⁴³ Treaty of 28 January 1988 between the United States of America and the Kingdom of Belgium on Mutual Legal Assistance in Criminal Matters (Belgium–USA MLAT), MB 8 December 1999 as amended by the Instrument visé par l’article 3, 2, de l’Accord entre l’Union européenne et les Etats-Unis d’Amérique en matière d’entraide judiciaire, fait le 25 juin 2003, concernant l’application de la Convention entre le Royaume de Belgique et les Etats-Unis d’Amérique concernant l’entraide judiciaire en matière pénale, signée le 28 janvier 1988, 16 December 2004, MB 8 March 2010.

²⁴⁴ Art. 1(2)(a) and (c) Belgium–USA MLAT.

²⁴⁵ Art. 17 Belgium–USA MLAT.

²⁴⁶ Art. 16 Belgium–USA MLAT.

²⁴⁷ Tosza, ‘Gathering Electronic Evidence: Mutual Legal Assistance’, 272.

²⁴⁸ R. A. Clarke, M. J. Morell, G. R. Stone, C. R. Sunstein and P. Swire, *Liberty and Security in a Changing World: Report and Recommendations of the President’s Review Group on Intelligence and Communications Technologies*, 12 December 2013, 227, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf. Also, for other MLAT procedures, see European Commission, ‘E-Evidence – Cross-Border Access To Electronic Evidence: Improving Cross-Border Access to Electronic Evidence’, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

²⁴⁹ Tosza, ‘Gathering Electronic Evidence: Mutual Legal Assistance’, 269; Conings and Royer, ‘Verzamelen digitaal bewijs in strafzaken’, 269.

²⁵⁰ Verbruggen and De Schepper, ‘Ontsnappen space invaders aan onze pacmannen?’, 164.

²⁵¹ European Commission, *Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace*, No. 15072/16, 2 December 2016, 5, <http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf>.

²⁵² Tosza, ‘Gathering Electronic Evidence: Mutual Legal Assistance’, 272–273.

²⁵³ European Commission, *Non-paper: Progress Report*.

²⁵⁴ Art. 7 Loi sur la transmission policière internationale de données à caractère personnel et d’informations à finalité judiciaire, l’entraide judiciaire internationale en matière pénale et modifiant l’article 90ter du Code d’instruction criminelle (Mutual Assistance in Criminal Matters Act), 9 December 2004, MB 24 December 2004.

9.4.2.2 Nature of the Cooperation

Kerkhofs and Van Linthout write that several foreign service providers are aware of their duty to cooperate and comply. Examples of those service providers are Parship GmbH (Germany), UPC Nederland, Planet Technologies (the Netherlands) and 2dehands.be (the Netherlands).²⁵⁵ The *Skype* and *Yahoo!* case law shows that some foreign service providers sometimes refuse to cooperate. An explanation could be possible conflict with the (privacy) legislation of their home state. Another reason, more economic in nature, could be that some enterprises refuse to cooperate because the costs of compliance in every country where services are offered largely surpass the costs of legal proceedings initiated against them in case of a refusal.²⁵⁶ A third reason might be that certain providers are unable to cooperate owing to technical restraints. WhatsApp, for instance, uses end-to-end encryption, which results in uncertainty as to whether it is able to recover the content of messages. Moreover, service providers are not always transparent about the information they preserve or have access to.

Cooperation also frequently takes place on a voluntary basis, although the scope of this mostly seems to be limited to non-content data (see also Section 9.4.2.1.3). Several providers (e.g. Apple, Google Inc., Facebook, Microsoft ...) cooperate upon simple request from the Belgian LEAs.²⁵⁷ They even prefer this technique rather than acknowledging that they are subject to cooperation duties under Belgian law.²⁵⁸ It also appears that WhatsApp and Facebook are more likely to voluntarily cooperate with Belgian LEAs if someone's life is at stake or when a case gets media attention.²⁵⁹ The willingness to cooperate voluntarily is thus certainly not unlimited. Service providers' voluntary cooperation with LEAs has also become more difficult owing to the implementation of General Data Protection Regulation (GDPR) requirements. There are no explicit legal rules regulating this voluntary form of cross-border cooperation. Belgium does, however, have a single point of contact (SPoC) for voluntary cooperation: the International Request team of the NTSU processes all incoming and outgoing requests for identification and historical data. The lack of a legal basis means that no guarantees are provided to safeguard the rights of data subjects. The policy of the specific service provider is then one of the only (limited) safeguards. Google, for instance, narrows a request when LEAs have formulated it too broadly in its opinion.²⁶⁰ However, the procedure is not transparent and makes Belgian LEAs dependent on the goodwill of foreign service providers.²⁶¹

As regards cooperation between LEAs and foreign service providers, transparency reports remain an important source for statistical data. These tend to reflect mainly direct requests for cooperation.²⁶² Since a clear-cut distinction between mandatory and voluntary cooperation is difficult to make in a Belgian context, it is likely that the reports include both forms of cooperation. In 2022, the success rate of the 5,042 outgoing Belgian requests for (mostly subscriber) data in the context of criminal investigations to Google, LinkedIn, Meta, Reddit, Snapchat and TikTok was 83 per cent.²⁶³ This was significantly higher than the average success

²⁵⁵ Kerkhofs and Van Linthout, *Cybercrime* 3.0, 665.

²⁵⁶ Ibid.

²⁵⁷ Ibid., 663–664.

²⁵⁸ Ibid., 664.

²⁵⁹ E. Bergmans, 'We zijn afhankelijk van de goodwill van enkele Amerikaanse bedrijven', *De Standaard*, 17 June 2019, www.standaard.be/plus/20190617/avond/optimized/5.

²⁶⁰ User data requests from around the world, Google, <https://transparencyreport.google.com/user-data/>.

²⁶¹ Tosza, 'Gathering Electronic Evidence: Mutual Legal Assistance', 275.

²⁶² SIRIUS, *SIRIUS EU Digital Evidence Situation Report: 3rd Annual Report* (The Hague: European Union Agency for Law Enforcement Cooperation (Europol), 3 December 2021), 54, www.europol.europa.eu/publications-events/publications/sirius-eu-digital-evidence-situation-report-3rd-annual-report-2021.

²⁶³ SIRIUS, *SIRIUS EU Electronic Evidence Situation Report* (The Hague: European Union Agency for Law Enforcement Cooperation (Europol), 18 December 2023), 66 and 69, www.europol.europa.eu/publications-events/publications/sirius-eu-electronic-evidence-situation-report-2023.

rate in the EU (73 per cent). It appears that having an SPoC contributes to that success.²⁶⁴ Google complied at least partly with 85 per cent of all²⁶⁵ (929) user data disclosure requests from July 2023 until December 2023.²⁶⁶ During the same period, Facebook complied at least partly with 82.39 per cent of all (1,238) data requests.²⁶⁷ In all other scenarios, indirect cooperation under the rules of mutual legal assistance is required.

Data obtained under domestic cooperation duties (Articles 46bis, 88bis and 90quater(2) CCP) can in principle be used as evidence (Section 9.1.2.2). Evidence collected through voluntary direct cooperation does not seem to create any issues regarding admissibility, but the same domestic rules are applicable. A Belgian judge should in principle assess the admissibility of evidence obtained under an MLAT or EIO procedure, taking into account the procedural requirements of the requested state (*locus regit actum*).²⁶⁸ A national judge can, however, always assess whether evidence was collected abroad in conformity with fundamental rights, such as the right to privacy.²⁶⁹ If the procedural requirements that are indispensable to protect these rights have not been complied with, evidence will be considered unlawful and contrary to Belgian public order.²⁷⁰ Regarding the right to privacy, the national judge will have to verify the existence of, for instance, a legal basis for the required investigative measure in the requested state and of sufficient procedural guarantees (e.g. the intervention of a judge or a requirement of proportionality).²⁷¹ Nonetheless, the conclusion that evidence is illegally gathered does not necessarily lead to exclusion. The criteria set out earlier (Section 9.1.2.2) will have to be applied to verify whether such evidence can be used in court,²⁷² and a mere violation of the (fundamental) rights to privacy and data protection is not enough.

9.4.2.3 Legal Remedies and Protection of Human Rights

On matters of direct cooperation with foreign service providers under Articles 46bis, 88bis and 90quater(2) CCP, we refer to Section 9.3.4. The same remedies are available for evidence obtained through cooperation under bilateral or supranational instruments.

The unregulated nature of voluntary cooperation unsurprisingly results in an unsatisfactory level of protection of human rights. Major foreign service providers often outline the procedure to be followed. Moreover, whether or not the data subject is informed of the cooperation depends on the policy of the service provider. Some major service providers (Apple, Facebook, Google, Microsoft, Twitter and Yahoo!) all seem to notify their customers when their data has been sought

²⁶⁴ Ibid., 68.

²⁶⁵ Not necessarily only those in the context of criminal investigations.

²⁶⁶ Google Service and Data Availability Report, 'Information on How Laws and Regulations Affect the Privacy and Security of Users, as Well as the Availability of Information on the Internet', Google, <https://transparencyreport.google.com/>.

²⁶⁷ Government Requests for User Data: Belgium, Meta, <https://transparency.facebook.com/government-data-requests/country/BE>.

²⁶⁸ Art. 9 Directive regarding the European Investigation Order; Art. 13 Mutual Assistance in Criminal Matters Act; D. Van Daele, 'België en de internationale samenwerking in strafzaken: een status quaestionis', in *Themis Straff(proces) recht* (Bruges: die Keure, 2007), 90.

²⁶⁹ Van Daele, 'België en internationale samenwerking in strafzaken', 91; B. De Smet, 'Registratie en lokalisatie van elektronische communicatie', in *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer* (Mechelen: Kluwer, 2019), 54.

²⁷⁰ De Smet, 'Registratie en lokalisatie van elektronische communicatie', 54; Cour de cassation, 6 April 2005, No. P.05.0218.F, ECLI:BE:CASS:2005:ARR.20050406.1. See also Cour de cassation, 8 May 2007, No. P.07.0129.N, ECLI:BE:CASS:2007:ARR.20070508.2.

²⁷¹ De Smet, 'Registratie en lokalisatie van elektronische communicatie', 56. See also Cour de cassation, 6 April 2005.

²⁷² Art. 13 Mutual Assistance in Criminal Matters Act; Art. 29 European Investigation Order Act. For an example, see Cour de cassation, 11 January 2022.

by LEAs save when the circumstances or those LEAs do not allow them to do so.²⁷³ The broad interpretation of territoriality by national jurisprudence combined with the obligation of secrecy under national law seems to create an incentive for foreign service providers not to notify their customers. In theory, doing so could sometimes result in criminal charges in Belgium.

9.4.3 *Cooperation of National Service Providers with Foreign LEAs*

Belgian service providers can limit their willingness to engage in voluntary cooperation by assessing requests in light of their terms of use. Voluntary transfers of data by Belgian service providers to LEAs of third countries (i.e. not members of the European Economic Area) also have to comply with the principles of the GDPR²⁷⁴ and can, in the absence of an adequacy decision²⁷⁵ or appropriate safeguards pursuant to Article 46 of the GDPR, take place only if one of the derogations under Article 49 of the GDPR applies. The situations where these derogations will be applicable are in fact rather limited.²⁷⁶

Moreover, the European Data Protection Board (EDPB) has clarified that ‘in situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to the existing MLAT or agreement’.²⁷⁷ This statement makes direct cooperation (both voluntary and mandatory) between Belgian service providers and LEAs of third countries even more questionable.

9.4.4 *Opportunities and Challenges Created by the EU e-Evidence Regulation*

On 17 April 2018, the European Commission proposed new legislation on e-evidence in the form of a Regulation and a Directive. After years of negotiations, both were finally adopted in July 2023. Under this section, we will focus on the Regulation (the e-Evidence Regulation), which will be applicable from 18 August 2026. It will introduce a form of direct cooperation between the LEAs of one EU country and service providers established or represented in another EU country. We will focus on some general principles and the impact on Belgian law here.

The Regulation applies to service providers offering services in the Union, and it uses a similar territorial connecting factor as the Belgian Court of Cassation in the *Yahoo!* and *Skype* judgments. This means that for European production and preservation orders, service providers offering services in the EU, but established or represented in another member state, fall under the e-Evidence Regulation. Under the Regulation, European production or preservation orders can be issued only for stored data. The possibility to keep and deliver future data to LEAs under a European production order is thus not provided for. This obviously reduces the effectiveness of the Regulation.²⁷⁸ For the real-time collection of traffic, location and content data, Articles 88bis and 90quater CCP and their broad territorial scope will therefore remain relevant.

²⁷³ Council of Europe, *Criminal Justice Access to Data in the Cloud: Cooperation with ‘Foreign’ Service Providers*, T-CY (3 May 2016) 2, 20–21; e.g. ‘Information for Law Enforcement Agencies’, Meta (Facebook), <https://about.meta.com/actions/safety/audiences/law/guidelines>.

²⁷⁴ Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016, No. L119/1.

²⁷⁵ Art. 45 GDPR.

²⁷⁶ See, e.g., EDPB, *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679*, adopted on 25 May 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

²⁷⁷ *Ibid.*, 5.

²⁷⁸ V. Franssen, ‘The European Commission’s e-Evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?’, European Law Blog, 12 October 2018, <https://europeanlawblog>

The Regulation further distinguishes between subscriber data and ‘data requested for the sole purpose of identifying the user’ on the one hand and traffic and content data on the other. A European production order for the former categories can be issued by a public prosecutor, whereas only a judge could validate the issuance of a European production order concerning the latter categories. Belgium does not have a separate category of ‘data requested for the sole purpose of identifying the user’: a production order under Article 46bis CCP arguably covers all types of data allowing identification of a subscriber or common user. The public prosecutor can issue such an order; no judicial intervention is required. For other types of data, an intervention of a judge (and sometimes even a judicial inquiry) is in principle mandatory under national law. The Belgian category of location data seems to be covered under the European category of traffic data.

The Regulation also introduces some grounds not to comply that service providers can invoke, such as immunities, privileges or there being a *de facto* impossibility of complying due to circumstances not attributable to the service provider (such as not having the data anymore). Examples given of the latter ground (the person whose data is sought is not their customer/the data has been lawfully deleted before receiving the order) seem to indicate that this is not a groundbreaking new rule. Such a ‘refusal’ seems already possible under Belgian law. Unlike Belgian law, the e-Evidence Regulation explicitly addresses potential conflicts between requests for cooperation and third country law.²⁷⁹

The conditions for the European preservation order differ, to some extent, from the Belgian rules on expedited preservation. For instance, ‘proportionality’ is added to the requirements to issue a European preservation order. Belgian law does not yet contain such an explicit mention of the proportionality of the measure. The Regulation also introduces a non-renewable time limit of sixty days, extendable by an additional thirty days. The obligation to preserve the data ceases after this period, unless a request for production is launched. Belgian legislation currently states that an incoming request for preservation is valid for ‘at least 60 days’ and domestic preservation can last for a (renewable) time period of up to ninety days. The obligation for the issuing authority to inform the service provider when preservation is no longer required will also be a novelty. Lastly, the domestic provisions apply to ‘all data stored, processed or transmitted by means of an IT system’, so they are broader than the provisions under the e-Evidence Regulation (Section 9.3.3.6).

Noteworthy is also that the targeted person has the right to be informed and the right to effective remedies as regards production orders under the e-Evidence Regulation. Any notification obligation and other involvement of the member state where the service provider is established or represented will be a (highly controversial, because excessively burdensome) novelty for Belgium as well.

Since unilateral direct cooperation with foreign service providers as regards production orders is already considered possible in Belgium and because of the widespread practice of voluntary cooperation, it can be safely assumed that, if it were up to Belgium, the Regulation would not completely replace the existing possibilities under domestic law. However, sticking too much to national rules which differ from the European standard might incur resistance from ISPs and a plurality of cooperation regimes for enterprises in an EU single market are likely to be challenged as a disproportionate exception to EU data protection law. If Belgium does not adjust its domestic law, the added value of the Regulation might be rather limited (mainly to the

[.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/](https://ec.europa.eu/justice/evidence/evidence-reform/evidence-reform-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/).

²⁷⁹ Art. 17 e-Evidence Regulation.

disclosure of content data?). If foreign ISPs invoke the existence of a formal, harmonised regime to abandon informal regimes of voluntary cooperation, the Regulation will become very important for practitioners. It therefore remains to be seen whether the new European framework will increase legal certainty or, by creating separate legal regimes, contribute to more legal uncertainty. As we have emphasised repeatedly, Belgium highly depends on the existing forms of cooperation, but is aware of the unsustainability of its approach (see Section 9.4.1). A stricter regime, especially one that comes with additional bureaucracy and slows down e-evidence gathering, would put the country's traditional faith in EU initiatives to the test. Nonetheless, at least for content data, the e-Evidence Regulation appears to form a substantial improvement and will therefore be warmly welcomed by Belgium.

9.5 CONCLUSION

The Belgian lawmakers have clearly taken the peculiarities of e-evidence into account, especially since 2016. The resulting legal regime is, however, anything but flawless. Some current difficulties as regards interpretation, conformity with supranational instruments and jurisprudence and practical application have been pointed out throughout this chapter. The CJEU torpedoed and sank Belgium's general data retention obligation, but the Belgian authorities seem to have clutched at straws in the CJEU's judgments to design special data retention rules. The practical result of the adoption of the 2022 Data Retention Act is a general data retention obligation in all but name that is unlikely to survive renewed CJEU scrutiny. In the meantime, Belgian (case) law time and time again refuses to ban the use of unlawfully retained and/or accessed data as evidence in criminal proceedings, at least for evidence gathered before the formal annulment of the 2016 Data Retention Act.

Belgium has quite a broad range of cooperation duties, *inter alia*, related to obtaining identification, traffic and location data, interception of (private) content data, preservation of data, targeted future retention of data, gaining access to data, copying or deleting data and blocking websites. In a domestic context, these can all be considered mandatory forms of cooperation. As regards the protection of fundamental rights, we have highlighted some issues, including the lack of a clear notification of cooperation to the data subject and the lack of sanctions when procedural guarantees are not complied with. The shift in focus from the way in which data is gathered to the intrusiveness determined by the amount and the type of data that is accessed and used has also not yet been made.

Owing to the broad interpretation of the territorial scope by the Court of Cassation, some Belgian domestic cooperation duties (production orders, interception of data and the covert search of an IT system) are also applicable in a cross-border context. The active targeting of consumers for economic activities, that is, where services are offered, is considered to be the relevant connecting factor in that regard. A small territory and limited economic and political weight have thus been compensated by an extensive interpretation of national jurisdiction, a pioneering approach and a pragmatism cheered by law enforcement frontline staff – and probably even some governments – in other, less outspoken states. To our knowledge, not a single state has formally issued a diplomatic protest against Belgian cross-border digital law enforcement, as could be expected if they felt there was a problem of sovereignty or violation of the fundamental rights of their subjects. Belgium sees itself as a trailblazer with respect to the extraterritorial application of domestic obligations to cooperate and may in the long run set the trend for future cooperation between friendly states, as the only answer to the perceived ineffectiveness and the time-consuming character of existing mutual legal assistance instruments.

However, upon closer watch, the tough unilateral legal chest-beating that has resulted in court battles tends to distort the picture: in day-to-day practice, voluntary cooperation between Belgian LEAs and foreign service providers is used in most cases. Statistical data shows that LEAs have a high chance of receiving a positive answer to their requests (for non-content data). The downside is that LEAs thus also highly rely upon this form of cooperation, and refusals by unwilling service providers frustrate both LEAs and cooperating competitors. A coherent, completely fundamental-rights-proof legal framework is, unfortunately, still lacking under domestic legislation.

So far, Belgium has not suffered a lot of prejudice because of its pride, but it remains to be seen whether the good cop/bad cop policy towards ISPs of the past years is effective in the long run, especially in relation to providers from non-Western states. There is broad consensus that a pan-EU regime, combined with better cooperation with the rest of the world, is necessary. Belgium therefore actively supports EU initiatives such as the e-Evidence Regulation, but whether that will achieve its intended objective remains to be seen. Maintaining the possibility of direct cooperation in a sufficiently effective way will in any case be vital for Belgian LEAs.

Digital Evidence in Estonia

Agnes Kasper, Eneli Laurits and Melita Sogomonjan*

10.1 INTRODUCTION

Estonia is an advanced e-state, where novel information and communication technology (ICT) solutions support the daily work of all sectors, including the public sector and the law enforcement authorities (LEAs).¹ It has also created the image of an innovative country with e-law regulating the provision and use of public services online.²

Furthermore, the use of ICT in criminal investigations has raised questions on the importance of digital evidence and gained significant interest concerning fundamental rights and the speed of the pre-trial investigation.³ In 2016, a fundamental reform began to fully digitalise criminal procedure and modernise the regulation of digital evidence in criminal proceedings.⁴ However, at present, Estonian law still does not include any specific regulations on digital evidence as such, and with high likelihood the situation will remain the same in the years to come. This is due to the ongoing reform efforts making the rules of criminal procedure technology-neutral,⁵ rather than establishing a specialised regime for digital evidence.

Current criminal procedure relies to a great extent on general and broad powers to meet the challenges of modern investigations. The Code of Criminal Procedure (CCP) dates from 2003 and is the result of the first thorough legal reform in this field after Estonia regained independence in 1991. While the importance of digital evidence in criminal proceedings is steadily increasing, the CCP does not define or provide specific procedures or principles relating to

* The contribution by A. Kasper is part of the cooperation within Jean Monnet Network ‘European Union and the Challenges of Modern Society’ (611293-EPP-1-2019-1-CZ-EPPJMO-NETWORK). The European Commission support to produce this publication does not constitute an endorsement of the content which reflects only the views of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

¹ T. Kerikmäe and S. Särav, ‘Legal Impediments in the EU to New Technologies in the Example of E-residency’ (2015) 8(2) *Baltic Journal of Law & Politics* 71–90.

² T. Evas, T. Hofmann, K. Joamets, R. Loik, K. Nyman-Metcalf, A. Popov and S. Särav, ‘General Frameworks’, in T. Kerikmäe, K. Joamets, J. Pleps, A. Rodina, T. Berkmanas and E. Gruodytė (eds.), *The Law of the Baltic State* (Cham: Springer, 2017), 40.

³ J. Ginter, A. Plekksepp, A. Soo, M. Kairjak, A. Kangur and T. Mets, *Analüüs isikute põhiõiguste tagamisest ja eeluurimise kiirusest kriminaalmenetluses* [An Analysis Ensuring Fundamental Rights of Individuals and the Speed of Preliminary Investigation in Criminal Proceedings] (Tartu: Tartu Ülikool, 2013), 178.

⁴ Republic of Estonia Ministry of Justice, *Kriminaalmenetluse seadustiku muutmise seaduse eelnõu väljatöötamise kavatsus* [Proposal of Amendments to the Code of Criminal Procedure], nr 8-1/1226 of 9 February 2017, <https://eelnoud.valitsus.ee/main/#/ljiBLVD9>.

⁵ Republic of Estonia Ministry of Justice, *Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse (kriminaalmenetluse seadustiku revisjon) eelnõu seletuskiri* [Explanatory Note to the Draft Law Amending the Code of Criminal Procedure and Other Laws (Revision of Code of Criminal Procedure)], nr 8-1/4367 of 17 July 2018, www.ekou.ee/doc/2019-07-17_JM-KrMS-revisjon-selk.pdf.

digital evidence. The general rules of evidence apply to evidence in digital form, and it is possible to submit digital evidence in criminal proceedings based on these rules.

In the aftermath of the 2007 cyberattacks against Estonia, it became clear that the then applicable rules of criminal law (combining the complications arising from the substantive and procedural laws) were not well-suited for investigating globally sourced large-scale cyberattacks. It was also acknowledged, however, that the high reliance of the entire society, including the development of an e-government, brought along significant new vulnerabilities, for which the state had to answer.⁶ Driven by its experience and security concerns, Estonia revised its criminal law rules, creating a system that does not place a disproportionate burden on law enforcement in procedural requirements to investigate incidents where attacks seem to originate from more than 100 countries by millions of hijacked devices. The system of rules created and adjusted for the purposes of fighting large-scale cyberattacks, however, has been subject to changes mainly due to judicial activity both at the domestic and at the European level, but also international and European legislative processes are underway that affect the collection of digital evidence. In recent years, external influences seem to dominate; while some of these are expected to ease the work of law enforcement, others end up fixing one detail and creating inconsistencies elsewhere. Estonia's concern is both for respect for fundamental rights and for ensuring security in all domains, including cyber. Therefore, when the (false) dichotomy of privacy versus security is relied on for suggesting or demanding changes in the system, prudence needs to be exercised by rule-makers.

10.2 SETTING THE SCENE

10.2.1 *Overview of Criminal Proceedings and Digital Evidence*

Article 31 (1) of the CCP defines that investigative authorities are, within their respective jurisdictions, the Police and Border Guard Board, the Internal Security Service, the Tax and Customs Board, the Competition Board, the Military Police, the Environment Board and the Department of Prisons of the Ministry of Justice and the prisons.⁷ Pre-trial proceedings are conducted by the Police and Border Guard Board and the Internal Security Service with some exceptions,⁸ and the former has investigative jurisdiction by default, unless otherwise provided by law.⁹

The investigative authorities perform the procedural operations provided in the CCP independently unless the permission of a court or the permission or order of the Prosecutor's Office is necessary. Investigative authorities have the right to demand submission of any document necessary for solving a criminal matter.¹⁰

When resolving a criminal matter, the court relies on facts which it has declared to be proven or a matter of common knowledge.¹¹ Facts relating to subject of proof are: (1) the time, place and manner of commission of the criminal offence and other facts relating to the criminal offence;

⁶ E. Tikk, K. Kaska and L. Vihul, *International Cyber Incidents – Legal Considerations* (Tallinn: CCD COE, 2010), 14–34, https://ccdcoe.org/uploads/2018/10/legalconsiderations_o.pdf.

⁷ Kriminaalmenetluse seadustik [Code of Criminal Procedure (CCP)], RT I 2003, 27, 166. In force since 1 January 2022.

⁸ CCP Art. 212(1).

⁹ Politsei- ja Piirivalveamet ja Kaitsepolitseiameti vaheline uurimisalluvus [Regulation on Investigative Jurisdiction between the Police and Border Guard Board and the Defense Police Board], RT I, 12.04.2013, 4; RT I, 07.05.2019, 4. In force since 10 May 2019.

¹⁰ CCP Art. 32(2).

¹¹ CCP Art. 60(1).

(2) the necessary elements of the criminal offence; (3) the guilt of the person who committed the criminal offence; and (4) information describing the person who committed the criminal offence, and other circumstances affecting the liability of the person.¹²

The Supreme Court has found that the Estonian system of proof requires clear differentiation between types of evidence, for example strict and free evidence, and the sources of evidence that are regulated by the CCP.¹³ Strict evidence is listed in Article 63(1) of the CCP and includes the statements of a suspect, accused and the victim, witness testimonies, expert reports and the statements given by an expert thereof, physical evidence, reports on investigative activities, minutes of court sessions, reports or video recordings on surveillance activities, and other documents, photographs, films or other data recordings. It should be noted that in the wording of Article 63(1), ‘other documents’ and ‘other recordings’ point to stored data. However, data can be collected in real time too during surveillance measures, in which case there will be a report or recordings of the data collected in transmission. Only strict evidence may be used in criminal proceedings to prove facts relating to a subject of proof set out in Article 62 of the CCP. Free evidence may be used for proving other facts related to criminal proceedings, for example procedural questions, to prove that a time limit was exceeded or that the search for fingerprints at a scene of an event took place as documented in the relevant report.

Estonian courts have found that short message service (SMS), emails but also voice recordings of one’s own conversations fall within the meaning of Article 63(1) of the CCP.¹⁴ Therefore, any message in digital form can be used as evidence if the terms of Article 64 of the CCP, containing the general conditions for evidence gathering, have been complied with. The only absolute prohibition on the use of evidence relates to cases where the requirements of law have not been complied with when applying for, or issuing, a permit for surveillance activities, or performing such activities.¹⁵

10.2.2 Terminology and Categorisations of Data

The term data is not legally defined under the Estonian national criminal procedure or in other legal acts. The CCP and the Electronic Communications Act (*Elektroonilise Side Seadus*¹⁶ or ECA) refer to two main categories of communications data: (1) subscriber data that is not related to the fact of communication (i.e., subscriber data); (2) data related to the fact of communication (i.e., traffic and location data). Furthermore, content data forms a separate category. This distinction is explained by the influence of EU law, in particular the Data Retention Directive.¹⁷ However, the terminology to denote these categories can be a source of confusion, relating to content data.

The ECA precisely refers to data revealing the content of communications (and that is excluded from retention obligation), whereas a specific term from the Constitution is used in the CCP – ‘messages transmitted’ – when it comes to investigative measures in criminal proceedings. According to case law, the dominant position currently is that content data can

¹² CCP Art. 62.

¹³ RKKKo (Judgment of the Criminal Law Chamber of the Supreme Court) 1 March 2006, 3-1-1-142-05, p. 10.

¹⁴ RKKKo 26 March 2009, 3-1-1-5-09, pp. 9 and 11.

¹⁵ CCP Art. 32(1).

¹⁶ *Elektroonilise Side Seadus* [Electronic Communications Act (ECA)], RT I 2004, 87, 593; RT I, 27.02.2022, 3. In force since 9 March 2022.

¹⁷ Council Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, OJ 2006 No. L105, 13 April 2006.

further be divided into content data in transmission and stored content data, whereas only the former enjoys the highest level of protection under Article 43 of the Constitution protecting the confidentiality of messages. This will be further explained in Section 10.2.4. Traffic and location data also falls outside the scope of Article 43 of the Constitution.¹⁸

Communication data subject to preservation (retention) by electronic communications undertakings is data which allows: (1) tracing and identification of the source of communication; (2) identification of the destination of communication; (3) identification of the date, time and duration of communication; (4) identification of the type of communications service; (5) identification of the terminal equipment or presumable terminal equipment of a user of communications services; (6) determining of the location of the terminal equipment.¹⁹ However, the extent of data retention obligation is in flux at the time of writing, as will be explained further in Section 10.3.6.

Access data such as passwords and decryption keys forms a separate, undefined category in Estonia and the Supreme Court has also referred to passwords as tools for enabling access to content of messages (stored in an email account in this case).²⁰ Passwords and decryption keys as such are not revealing about the content of communications either and cannot be said to belong to the essence of content;²¹ further, although they may be used to directly or indirectly identify a particular subscriber, they can also be changed.

10.2.3 *Investigative Measures*

Estonia signed the Cybercrime (CC) Convention on 23 November 2001 and ratified it on 12 May 2003. Estonia has not made reservations to the Convention. The provisions of the CC Convention have been satisfactorily implemented, although the CCP does not expressly provide for all specific measures listed in the CC Convention.

Article 16 of the Convention, dealing with expedited preservation of stored computer data, is implemented in Article 215 of the CCP, which imposes a general obligation to comply with the demands and orders of relevant authorities in criminal investigations – and which therefore remains relevant for other investigative measures also. Article 17 of the Convention, on expedited preservation and partial disclosure of traffic data, is covered by the same Article 215 of the CCP, as well as Article 90¹ of the CCP dealing with requests to electronic undertakings to submit information. Article 111¹ and 112 of the ECA, on data retention in the electronic communications sector and on the obligation of electronic communications undertakings to provide information, respectively, are also relevant in the implementation of Article 17 of the Convention. Article 18 of the Convention on production order is implemented in Article 91 of the CCP dealing with searches (complemented with provisions on inspection addressed in Article 86 of the CCP) and by rules on covert measures, in particular covert examination of things pursuant to Article 126⁵ of the CCP.

Table 10.1 summarises how different categories of data are collected, by which measures and whose authorisation is necessary for the collection.

It should be emphasised at the outset that Article 215 of the CCP generally requires compliance with orders and demands issued by investigative bodies and the Prosecutor's Office in the

¹⁸ According to Art. 43 of the Constitution of the Republic of Estonia, everyone has the right to confidentiality of messages sent or received by him or her by post, telegraph, telephone or other commonly used means. Derogations from this right may be made in the cases and pursuant to a procedure provided by law if they are authorised by a court and if they are necessary to prevent a criminal offence or to ascertain the truth in a criminal case.

¹⁹ ECA Art. 111¹(1).

²⁰ RKKKo 20 November 2015, 3-1-1-93-15, p. 102.

²¹ Ü. Madise, H. Kalmo, L. Mäliksoo, R. Narits, P. Pruks, J. Raidla and P. Vinkel, 'Eesti Vabariigi põhiseadus: kommenteeritud väljaanne' (2017) *Juura* Art. 42.2.

TABLE 10.1 *Data collection authorisations in investigations*

Data	Collection		Authorisation by	
Message content in transmission	Surveillance measures: wiretap and covert observation of information		Pre-trial judge	
Stored message content	(A) Surveillance measures: covert examination of a thing	(B) Covert entry may be also needed for (A), which should be authorised separately	(A) Prosecutor	(B) Covert entry is authorised by pre-trial judge
	Search		Pre-trial judge authorises seizure of electronic devices	
	Inspection		No authorisation required Measure conducted by investigative authority upon its own decision	
	Art. 215 CCP general request		Prosecutor/investigative authority	
Traffic and location data	Retained according to the ECA Data request under Art. 90 ¹ CCP		Pre-trial judge/court	

criminal proceedings conducted by them, and therefore Estonia does not have a specific investigative measure for each provision that can be found in the Council of Europe Cybercrime Convention.²² For example, Article 215 can be relied upon for ordering expedited preservation of stored computer data or for a production order to the extent that the issue is not covered by some other specific provision. However, Article 215 of the CCP is not applied to foreign service providers offering their services in Estonia.

Taking of evidence in criminal proceedings can be performed by means of public investigative measures (in the meaning that they are non-secretive measures) or surveillance activities (secretive ones). The most frequently used public investigative measures for the collection of digital data are searches, inspections and inquiries by bodies conducting proceedings to electronic communications undertakings to provide data.²³ Furthermore, surveillance activities denote the processing of personal data for the performance of a duty provided by law with the objective of hiding the fact and content of data processing from the data subject.²⁴

The provisions of the CCP on search set limitations in time and clearly refer to physical locations only. Places where the investigator could only step on virtually, like parts of a server, are not considered to be places to search. Search generally requires a judicial warrant, which sets out the object to be found, the reasons for the search and the place where the search is to be conducted.²⁵ Digital evidence is regarded as a document and finding a document can be the objective of a search. Thus, digital evidence can be seized as a document during a search.²⁶

²² Council of Europe, Convention on Cybercrime, ETS 185, 23 November 2001.

²³ CCP Arts. 91 and 83.

²⁴ CCP Art. 126¹(1).

²⁵ CCP Art. 91(4).

²⁶ According to Art. 91(1) of the CCP, the objective of a search is to find an object to be confiscated or used as physical evidence, a document, thing or person necessary for the adjudication of a criminal matter, assets to be seized in criminal proceedings or a body or to apprehend a fugitive in a building, room, vehicle or enclosed area. A search may be conducted if there is reasonable doubt that the object to be found is at the place of the search.

Inspection can be used to examine a document or any other object or physical evidence. Its objective is to collect information necessary for the adjudication of a criminal matter, detect the evidentiary traces of the criminal offence and confiscate objects which can be used as physical evidence.²⁷ Inspection is not limited in time and the authority conducting the proceedings does not have to obtain a warrant or define what is to be found or substantiate the reasons for conducting an inspection in advance. Article 87 of the CCP merely requires that an inspection report is prepared which sets out the findings in a descriptive manner. Searches of data mediums are performed as an inspection and, despite the obvious similarities between searching one's home and searching one's digital devices, currently there are no specific safeguards to guarantee the proportionality of interference with privacy when data mediums are examined during criminal proceedings. However, the *ultima ratio* principle remains generally applicable to collection of evidence.

To find digital evidence, the two above investigative measures can be combined, which has yielded effective practical results. According to Article 95 of the CCP, the investigative authorities seize a data medium during a search and can examine its content in the form of an inspection or an expert assessment. This approach has been approved by the Supreme Court, which held that a search and inspection are the appropriate measures to collect stored messages as evidence.²⁸

Nevertheless, the lack of clarity about some formal requirements of strict evidence has led to controversial practice, where digital evidence or its authentic copy is not added to the criminal file or presented to the court as evidence. Instead, the inspection report is used as evidence. This is because digital evidence can fall into the categories of 'physical evidence' (because stored on a data carrier), 'other document' or 'other data recording' under Article 63(1) of the CCP and often the rules of physical evidence were interpreted so as to require an inspection report about recordings. There is currently no guidance on the format in which such digital evidence should be presented to the court (e.g., on the probative value of a digital copy). On the other hand, a document containing information concerning the facts relating to a subject of proof may be used for the purposes of proof.²⁹ Apparently, the use of inspection reports (i.e., which are certainly documents) was a more straightforward way to go so far. The CCP is set for a change at this point, since a proposed amendment of the CCP defines the concept of a document and includes all sorts of data recordings regardless of (the type of) data carrier (paper, videotape, clay tablet, file on a hard disk or email on a server, etc.).³⁰ Documentary evidence will be clearly distinguished from physical evidence based on where the probative/value lies – in the recorded data or the individual properties of the physical object (e.g., shape, place, chemical composition, etc.).

Besides the above general investigative measures, Article 90¹ of the CCP also provides specific powers to request certain categories of data from electronic communications undertakings. Subscriber information can be requested by a body conducting proceedings such as courts, prosecutors' offices and investigative authority without the need for permission from a prosecutor or court. However, investigative authorities may request any data preserved according to the ECA (i.e., traffic and location data),³¹ on the condition that an inquiry is authorised by the court.

²⁷ CCP Art. 83(1).

²⁸ RKKKo 30 June 2014, 3-1-14-14, p. 817.

²⁹ CCP Art. 123.

³⁰ *Explanatory Note to the Draft Law Amending the Code of Criminal Procedure and Other Laws (Revision of Code of Criminal Procedure)*, 1.

³¹ ECA Arts. 111¹(2) and (3).

In addition to the previously discussed public investigative measures, the CCP provides legal ground for collecting digital evidence via surveillance measures. Article 126³ of the CCP provides that a surveillance agency may covertly observe or wiretap information, covertly enter a computer system, watch a person, thing or area, covertly take comparative samples and perform initial examinations, covertly examine an area or thing and covertly replace it. Permission of a pre-trial judge is a precondition for covert entry into computer systems, covert observation and wiretapping of information,³² while the prosecutor's authorisation is sufficient for covert examination of things or areas.³³ The Supreme Court clarified that the previous provisions differentiate between data being in the process of transmission (real time) and stored data (e.g., covert examination of part of a server storing an email message).³⁴ Surveillance activities are permitted on the bases stipulated by the CCP if collection of data by other activities or taking of evidence by other procedural acts is impossible, is impossible on time or is especially complicated or if this may damage the interests of the criminal proceedings.³⁵ The ECA complements the CCP's provisions on surveillance by obliging electronic communications undertakings to make it possible for authorities to conduct surveillance activities or restrict the right to confidentiality of messages in their communication networks upon request.³⁶

10.2.4 Data Retention Obligations: Legal Framework, Practice and Challenges

Estonia implemented the Data Retention Directive³⁷ in 2008 and, as a result, indiscriminate mass data retention is applied in the electronic communications sector, although recent adjustments were adopted in line with EU case law (see Section 10.2.5.3). The ECA divides electronic communication services into different categories, and these are used to differentiate between the personal scope of data retention provisions. The act defines communications undertakings, as providers of telephone or mobile telephone services, telephone network and mobile telephone network services, and providers of internet access, electronic mail and internet telephony services.

The ECA prescribes that all communications undertakings retain their users' traffic and location without further distinction based on the seriousness of offence, identity or status of user or other criteria.³⁸ Data is retained for a one-year term, which can be prolonged by the government for a limited period and in the interest of public order or national security.³⁹

While the general data retention obligation applies to all electronic communications undertakings, separate provisions detail the precise type of data to be retained by service providers in the telephony field and internet-based communications (i.e., internet access, email and internet telephony).⁴⁰ Although in recent judgments the Court of Justice of the European Union (CJEU) ruled, inter alia, that data retention obligations concerning telephony services should be set aside due to conflict with EU law (see Section 10.2.5.3), there are no changes in the general practice.

Data retained by these specific service providers must remain in the territory of an EU member state. However, inquiries and information provided in response, as well as some logs,

³² CCP Arts. 126³ and 126⁷.

³³ CCP Art. 126⁵.

³⁴ RKKKo 20 November 2015, p. 92.

³⁵ CCP Art. 126³(2).

³⁶ ECA Art. 113(1).

³⁷ Council Directive 2006/24/EC.

³⁸ ECA Art. 111¹(1).

³⁹ ECA Art. 111¹.

⁴⁰ ECA Arts. 111¹(2) and 111¹(3).

must be preserved in the territory of Estonia.⁴¹ Communications undertakings must ensure the protection and security of retained data, as well as restrict access to the data. It is also clarified that the content of messages (such as emails or phone calls) is not recorded, and that no data revealing the content of communications is preserved.⁴²

10.2.5 Case Law

In 2014 and 2015 the Supreme Court delivered two landmark decisions⁴³ that have proven to be foundational for Estonia's approach to digital evidence. These cases clarify that only messages (including emails) in the process of transmission can be intercepted, and that the copying of emails that have already arrived at the addressee is not interception. Copying or accessing and viewing stored messages can conceptually be inspection, examination or observation of the part of the physical device where such messages are stored, regardless of the location of the storage device. However, in 2021 another highly influential case was also concluded, based on the CJEU's preliminary ruling in *Prokuratuur*,⁴⁴ which provoked plenty of reactions and intensified discussion about the protection of fundamental rights, and which resulted in some changes in the data retention regime.⁴⁵ These cases will be discussed in more detail next.

10.2.5.1 The 2014 Case of *Reiljan and others* on the Status of Stored Messages

The case of *Reiljan and others* was one in a series of corruption-related cases involving high-profile politicians and businessmen, and, in terms of evidence, it was very complex.⁴⁶ Evidence relied on by the prosecution included emails that were found in computers after those had been taken away during a search. The defendant argued that copying data from such computers without the permission of a pre-trial judge is unlawful, because all messages are protected by Article 43 of the Constitution.⁴⁷

The court, however, disagreed and explained the scope of protection of Article 43 of the Constitution, therefore essentially distinguishing between data in transmission and stored data, and consequently clarifying the scope of interception, search and inspection. The court held that Article 43 of the Constitution protects only those messages that are in the process of communication. Messages that are stored on a data carrier and that are in the possession of the sender, or the recipient, are excluded from the scope of protection. Article 43 of the Constitution directly refers to messages in transmission, and not just any message. The protection of the right to confidentiality of messages provided by Article 43 of the Constitution extends to emails or SMS messages from their sending until the arrival at the addressee, similarly to telephone conversations during the time they are taking place, as well as to postal items from the moment of conveyance to postal services until the delivery to the addressee. This is justified because messages in transmission are outside the sphere of influence of the sender and the addressee and cannot be protected from third persons. Once a message has arrived at the addressee, that person can decide to delete or render it unavailable

⁴¹ ECA Art. 111¹(5).

⁴² ECA Art. 111¹(9).

⁴³ RKKKo 30 June 2014 and RKKKo 20 November 2015.

⁴⁴ Case C-746/18, *H.K. v. Prokuratuur* [2021] ECLI:EU:C:2021:152.

⁴⁵ RKKKo 18 June 2021, 1-16-6179.

⁴⁶ RKKKo 30 June 2014, p. 622.

⁴⁷ Eesti Vabariigi põhiseadus, RT I 1992, 26, 349; RT I, 15 May 2015, 2.

to third persons by other means. Therefore, the court's permission is not needed to copy a message that has already arrived at the addressee and this operation can be performed based on the provisions on search and inspection.⁴⁸

10.2.5.2 *Onksion and others* on Illegal Private Surveillance

Another corruption-related case, *Onksion and others*,⁴⁹ ending in conviction of the Centre Party as well as two Members of the Parliament, revolved around unauthorised surveillance and violation of confidentiality of messages. However, this time the messages in question were stored on Gmail servers.

To access H.R.'s Gmail account, Mr Onksion used H.R.'s credentials, which were saved in the memory of Onksion's work laptop by mistake (for a short period H.R. and others were using Onksion's computer due to technical issues at the office). Onksion noticed and used this opportunity to repeatedly enter H.R.'s account and forward or print out and hand over H.R.'s messages to Centre Party politicians. Without distinguishing between the locations of the devices where the messages are stored, the court went on to consider whether such conduct can amount to unauthorised surveillance and violation of confidentiality of messages. The court found that Onksion's conduct is covert examination of things as referred to in Article 126⁵ of the CCP, which is a surveillance measure. The service provider's server is a thing, and Onksion was secretly examining the server's part that contained H.R.'s emails without authorisation. However, Onksion's conduct did not amount to interception (i.e., wiretapping), partly because that would presume the real-time processing of messages in transmission, and such real-time processing did not take place.

In considering the violation of confidentiality of messages, the court decided that Onksion's conduct was not interference with messages in transmission;⁵⁰ thus, the protection of Article 43 of the Constitution did not apply. However, the court also considered the application of Article 26 of the Constitution on the inviolability of privacy and family life, which does not differentiate between stored data and data en route. Article 26 is applicable to traffic data and stored content of messages, but it entails lower-level safeguards than those afforded under Article 43.

In the current case, the court found misuse of security elements of the account owner by Onksion, but the risk of such misuse does not arise from lack of control over confidentiality of messages during the communication process. The messages in question had already completed the phase of communication that is outside the control of the email account's owner (H.R.); thus, there was no violation of confidentiality of messages. The court, however, noted that a violation of confidentiality of messages could take place, for instance, using a copy recorded at the service provider transmitting the message.⁵¹

Yet, not all jurists agree with this narrow interpretation⁵² and one justice of the Supreme Court offered a dissenting opinion.⁵³ The issue is whether the approach to confidentiality of messages as laid down in the Constitution reflects the actual need for protection in the technological environment of the twenty-first century, and whether it is reasonable to provide protection for messages only at the time of their transmission (see further in Section 10.3.5).

⁴⁸ RKKKo 30 June 2014, p. 816.

⁴⁹ RKKKo 20 November 2015.

⁵⁰ RKKKo 20 November 2015, pp. 102–104.

⁵¹ RKKKo 30 June 2014, p. 103.

⁵² U. Lõhmus, 'Once More about Messages' Confidentiality or What Impact the 20th Century Technology Has on the Fundamental Law's Interpretations' (2016) 3 *Juridica* 175–183.

⁵³ Dissenting opinion of Judge E. Kergandberg on judgment of RKKKo 20 November 2015, 3-1-1-93-15.

The case of *Onksion and others* has also been instructive on questions of admissibility, and even more so since the server owner and entity receiving a request for documents (emails) was the Chancellery of the Riigikogu (i.e., the Estonian Parliament). The investigative authority relied on the general power to demand production of emails according to Articles 32(2) of the CCP and the general obligation to comply with such demands under Article 215(1) of the CCP. The requested emails were the ones forwarded by Onksion from H.R.'s email account to L.L.'s email account, L.L. being a Member of the Parliament at the time.

The defendant argued that the requested emails should be inadmissible because the Chancellery does not have the right to disclose L.L.'s emails to the investigative authorities, since there is no subordination relationship between them, nor any legal or contractual basis for processing the emails. Use of email is protected by provisions relating to privacy. Yet the court held that the CCP provisions apply independently and regardless of the relationship between the user email account and the server owner. Contractual obligations or one-sided declarations cannot alter the obligations of subjects arising from criminal proceedings.⁵⁴

10.2.5.3 The Case of *Kuusmaa* and the CJEU's *Prokuratuur*

The *Kuusmaa* case became locally known as the 'dog sausage case', since the plot involves stealing of chocolate, marmalade, dog sausages, onion, garlic, cash and so on from private dwellings, but also computer-related fraud by K.⁵⁵ The investigative authority requested retained traffic and location data from an electronic communications undertaking regarding K's communications and used the provided data to prove the theft and the fraud. The defendant challenged the use of retained traffic and location data, arguing that the reports based on these are not admissible and relying on the CJEU's *Tele2 Sverige* ruling.⁵⁶ The Supreme Court referred the case to the CJEU for preliminary ruling. The well-known questions, reasoning and outcome of the consequent CJEU's *Prokuratuur*⁵⁷ case are not discussed here,⁵⁸ but rather attention is paid to the case's reception at national level.

In the Estonian Supreme Court's summary of *Prokuratuur*, the CJEU explained that the e-Privacy Directive⁵⁹ precludes national legislative measures that proactively oblige providers of electronic communications services to retain traffic and location data in general and without distinction.⁶⁰ The Estonian court further explained in its decision that, based on the practice of the CJEU, it can be stated that the retention of and access to communications data constitute separate infringements of the rights protected by the Charter, and the general and indiscriminate retention of communications data is not permissible even if strict substantive and procedural requirements for access to data are established by law. Both the retention of and access to communications data must be proportionate.⁶¹ The high court unequivocally stated that Article 111¹(2) of the ECA, which requires the indiscriminate mass retention of traffic and location data by the providers of telephone or mobile telephone services and telephone network and mobile

⁵⁴ RKKKo 20 November 2015, p. 64.

⁵⁵ RKKKo 18 June 2021.

⁵⁶ Case C-203/15, *Tele2 Sverige AB v. Post-och telestyrelsen* and Case C-698/15, *Secretary of State for the Home Department v. Tom Watson and others* [2016] ECLI:EU:C:2016:970.

⁵⁷ *H.K. v. Prokuratuur*.

⁵⁸ For detailed analysis of the case, see, e.g., Ioannis Revolidis, 'H.K. v Prokuratuur: On Balancing Crime Investigation and Data Protection' (2020) 6(2) *European Data Protection Law Review* 319.

⁵⁹ Directive 2002/58/EC of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications), OJ 2002 No. L201, 31 July 2002.

⁶⁰ RKKKo 30 June 2014, p. 24.

⁶¹ *Ibid.*, p. 43.

telephone network services, is in conflict with EU law.⁶² For these reasons, both Article 111¹(2) of the ECA requiring the mass collection of traffic and location data, and the CCP provision allowing requests to be made for the same data, should be set aside and not be applied.⁶³

In September 2021 the Association of Information Technology and Telecommunications requested guidance regarding the court decision. The Ministry of Justice responded that, in its interpretation, the court set aside the conflicting rule of Article 111¹(2) of the ECA for the purposes of the case, but it does not automatically mean that the provision would not be valid. Moreover, the Ministry noted that there is no clarity on the interpretation of the CJEU ruling at EU member state level and that there are member states where a general and uniform retention regime for communications data continues to be in place.⁶⁴

Meanwhile, the Estonian legislator has adopted steps that address some of the questions raised in *Kuusmaa* and *Prokuratuur*. Amendments to the CCP adjusted the conditions for requesting and accessing retained traffic and location data from electronic communications undertakings and they entered into force on 1 January 2022 (see Section 10.2.3). However, one should also note that the court did not address Article 111¹(3) of the ECA, which requires the retention of traffic and location data by providers of internet access, electronic mail and internet telephony services. Moreover, no changes have been made to date to Article 111¹(2) of the ECA.

10.3 DOMESTIC COOPERATION BETWEEN LEAs AND SERVICE PROVIDERS

In terms of the Council of Europe Cybercrime Convention, the CCP applies to both types of service providers, the ones that provide the ability to communicate by electronic means, and the ones whose service is processing or storing computer data.⁶⁵ This is achieved as the CCP refers specifically only to electronic communications undertakings (within the meaning of the ECA), thereby singling them out from all possible (digital) service providers.⁶⁶ This distinction is also reflected in prescribing specific cooperation duties for electronic communications undertakings, but also having in place a general cooperation duty that covers everyone, including any other service providers, and applies in the territory of Estonia.⁶⁷

Pursuant to the ECA, electronic communications undertaking means a person who provides publicly available electronic communications services to the end-user or to another provider of publicly available electronic communications services.⁶⁸ Publicly available electronic communications services, according to the new definition based on the European Electronic Communications Code,⁶⁹ are services provided under agreed conditions on electronic communications networks, being internet access services, interpersonal communications services, or other services that consist wholly or mainly in the conveyance of signals, but that are not media services.⁷⁰

The cooperation of service providers and Estonian LEAs has been great throughout the years. Private sector companies answer law enforcement agencies' data requests either

⁶² Ibid., p. 45.

⁶³ Ibid., p. 49.

⁶⁴ Ministry of Justice, 'Vastus pöördumisele' [A Response to Appeal], No. 10-4/5771-2, 30 November 2021.

⁶⁵ Convention on Cybercrime, Art. 1(c).

⁶⁶ CCP Art. 90¹.

⁶⁷ CCP Art. 215.

⁶⁸ ECA Art. 2(5).

⁶⁹ Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code, OJ 2018 No. L321, 17 December 2018.

⁷⁰ ECA Art. 2(6).

voluntarily or according to Articles 215 and 90¹ of the CCP. As a rule, requests are answered within two weeks or faster if necessary.⁷¹

10.3.1 *Principles Applicable to the Investigation of Offences*

A general principle for the territorial and temporal applicability of the CCP is set out in Article 3, pursuant to which the criminal procedural law applies in the territory of Estonia. Estonian criminal procedural law applies to criminal proceedings conducted in Estonia, regardless of the place of the offence. However, there are two exceptions to this general rule. The first exception is related to the state of emergency, while the second is related to the use of evidence collected abroad which is gathered based on the mutual recognition principle, that is, the framework of cross-border cooperation between authorities in the criminal sphere.⁷² Thus, the application of foreign criminal procedure is accepted for the purposes of collection of evidence.⁷³

Once the applicability of the Estonian criminal procedure is ascertained, it applies equally to all persons with some exceptions of high offices and persons enjoying diplomatic or other privileges.⁷⁴ As a general rule, everyone in the territory of Estonia is obliged to comply with the orders and demands of investigative authorities and the Prosecutor's Office in criminal proceedings.⁷⁵

The complex problem of jurisdiction is simple in practice and the first step is to identify the locations where the evidence is held to make requests to acquire log data or request its storage. Depending on the location, international channels may also be used if needed. Search of computer systems is not regulated as such, but, using the search and/or inspection provisions, data can be accessed in the territory of Estonia, regardless of the actual location. During the inspection of, for instance, a social media website, a subject may cooperate (disclose usernames and passwords). Nevertheless, cooperation is not always provided.⁷⁶

Courts have left the investigative jurisdiction question open and little debate is ongoing. There is uncertainty around which factors should be taken into consideration when determining jurisdiction. Is it due to the 'loss of location' (and how far one should go trying to ascertain the location) or to the location of the headquarters of the company (i.e., Google or Facebook)? In fact, covert measures account for some part of the activities, but they do not solve all the problems and therefore computers are mostly searched by applying public investigative measures.⁷⁷ Claims about Estonian jurisdiction over data stored in foreign territories were accepted by pre-trial judges,⁷⁸ and currently there are no indications that prosecutors or investigative agencies will need to apply a more restrictive approach any time soon.

⁷¹ Council of the European Union, *Evaluation Report on the Seventh Round of Mutual Evaluations: The Practical Implementation and Operation of European Policies on Prevention and Combating Cybercrime, Report on Estonia*, 10953/15, 5 April 2016, p. 26.

⁷² E. Kergandberg and P. Pikamäe, *Kriminaalmenetluse Seadustik – Kommenteeritud Väljaanne* (Tallinn: Juura, 2012), 49.

⁷³ *Ibid.*, 48, 225.

⁷⁴ CCP Art. 4.

⁷⁵ CCP Art. 215.

⁷⁶ E. Laurits, 'Some Problems Encountered in Computer System Searches', in M. Möttus (ed.), *Yearbook of Estonian Courts* (Estonia: Dada, 2015), 150.

⁷⁷ *Ibid.*, 151.

⁷⁸ E. Laurits, 'Criminal Procedure and Digital Evidence in Estonia' (2016) 13 *Digital Evidence and Electronic Signature Law Review* 113–120.

10.3.2 Overview of Existing Cooperation Duties

National service providers cooperate with investigative agencies on a mandatory legal basis. Cooperation with domestic service providers reportedly functions smoothly and often they are the first ones to be turned to in investigations.

10.3.2.1 Public Investigative Measures

For the collection of digital evidence, the most often used measures are public investigative measures, search and inspection. These were discussed in Section 10.2.3. The general cooperation duty set out in Article 215 of the CCP applies to service providers in this respect. Since these general measures are formulated in a technology-neutral manner, they also apply as cooperation duties of service providers.

Those service providers which qualify as electronic communications undertakings under the ECA are also obliged to provide retained communications data upon the request of the investigative authority conducting proceedings based on Article 90¹ of the CCP. However, this cooperation duty can be relied on for investigating offences for which the CCP allows surveillance measures,⁷⁹ or when it is inescapably necessary for achieving the purpose of criminal proceedings, it is justified by the gravity and nature of the offence, and it does not unjustifiably interfere with personal rights.⁸⁰

The limitation of the data requests to investigation of serious crimes is a recent addition to the CCP based on the CJEU's decision in *Prokuratuur*.⁸¹ The case revolved around two main issues: firstly, the purposes for which requests for retained data can be made to electronic communications undertakings; and secondly, the power to authorise such requests. Prior to the ruling, data requests were allowed for any offence, although the *ultima ratio* principle applied, and the permission of the Prosecutor's Office was sufficient, despite that it directs the pre-trial proceedings and brings the public prosecution before the court. The European court held that, given this role of the Prosecutor's Office, it could not be independent.⁸² The CCP was also supplemented with the requirement that, in addition to the unavoidable necessity, the gravity and nature of the criminal offence and the violation of personal rights accompanying the request must be considered when granting permission for communications data. Consequently, since 1 January 2022, the pre-trial judge's permission is required to request retained traffic and location data from electronic communication undertakings, but subscriber data can still be requested by authorities conducting the proceedings without specific approval.

Requests for subscriber information can also be submitted to electronic communications undertakings orally, confirming the authenticity of the request by a password, and if other data is requested, then in writing or in electronic form.⁸³ The electronic communications undertaking answers the request or grants access to the requested information as soon as possible if the case is urgent, but no later than within ten hours. In other cases, the request is answered within ten days.⁸⁴

The electronic communications undertaking is merely a technological intermediary and attention is paid to keep data confidential as much as possible when needed, also respecting the principles of privacy and personal data protection. Hence, it is at least expected by data

⁷⁹ CCP Art. 126²(2).

⁸⁰ CCP Art. 90¹(3).

⁸¹ *H.K. v. Prokuratuur*.

⁸² *H.K. v. Prokuratuur*.

⁸³ ECA Art. 112(2).

⁸⁴ ECA Art. 112(1).

subjects that service providers' employees should not see the requested information if a viable solution exists for that. Access to retained data may be ensured by the communications undertaking, based on a written contract, by way of continuous electronic connection.⁸⁵

10.3.2.2 Covert Measures (Surveillance) in the CCP

Surveillance activities may be conducted with the written permission of a pre-trial judge or the Prosecutor's Office. The CCP contains a catalogue of more than 150 offences in case of which surveillance measures can be applied.⁸⁶ This list is composed by considering four factors: whether it is a hidden offence, the time span, whether it is the preserve of organised crime, and the priority level for the state.

Article 126⁷ of the CCP regulates wiretapping or covert observation of information. However, this section applies only to messages or information in transmission; hence, when an email or other communication has arrived at the recipient's inbox, or has been stored in a similar manner, examination of those messages falls outside the scope of this provision. The case of *Reiljan and others* described in Section 10.2.5.1 illustrates this point.

Article 126⁷ also applies to covert observation of internet traffic⁸⁷ and data flows in digital devices. Service providers have no specific obligation to facilitate such covert measures; for example, service providers do not install and/or operate spyware on their clients' devices upon the request of surveillance authorities under the CCP. To conduct covert observation of internet traffic, authorities would need to use special-purpose software that forwards the required information from the device under surveillance. If covert entry into a computer system is necessary to install or remove technical appliances necessary for surveillance, the Prosecutor's Office needs to apply for permission from a pre-trial judge for the covert entry and wiretap or the covert observation of information separately. In 2021, 890 permissions were issued for wiretap and covert observation of information other than telephone wiretap, while the total number of new authorised surveillance measures was 1,360.⁸⁸

Any surveillance agency can also covertly examine a thing (i.e., digital device or part of it, such as the case with email accounts), whereas under the CCP wiretap is reserved for the Police and Border Guard Board, the Internal Security Service and the Prisons Department. However, in the context of collecting digital data, the provisions of Article 126⁵ on covert examination are the more relevant.

Covert examination can be authorised by the Prosecutor's Office for up to two months. During covert examination it is not permitted to violate confidentiality of transmitted messages, so it is not permitted to eavesdrop on conversations or record data in transmission. Covert examination of a digital device can be done by having either direct or remote access to a device, or to part of a device. How this can technically take place is illustrated by the 2015 case (*Onksion and others*) discussed in Section 10.2.5.2, where the (accidentally) saved username and password were used to covertly enter and examine an email account.

⁸⁵ ECA Art. 112(2).

⁸⁶ CCP Art. 126²(2).

⁸⁷ N. Aas, *Riigi peaprokuröri ülevaade Riigikogu põhiseaduskomisjonile seadusega prokuratuurile pandud ülesannete täitmise kohta 2013* [The Chief Prosecutor's overview to the Constitutional Committee of the Parliament on the fulfilment of the tasks assigned to the Prosecutor's Office by law in 2013] (Tallinn: Prosecutor's Office, 2014), 22, www.prokuratuur.ee/sites/default/files/pressiteated-failid/riigi_peaprokurori_ettekanne_pohiseaduskomisjoni_2013_o.pdf.

⁸⁸ Prokuratuuri Aastaraamat [Yearbook of the Prosecutor's Office], Dilaila Nahkur-Tammiksaar, Kriminaalmenetluse statistika ['Criminal Procedure Statistics'] (2021), <https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2021/kriminaalmenetluse-statistika>.

10.3.2.3 Cooperation Duties in the ECA to Support Surveillance (Covert Measures)

The CCP's provisions on surveillance are supported by Article 113 of the ECA. It lays down the obligation of electronic communications undertakings to grant a surveillance agency or security authority access to communications networks for conducting surveillance activities or for the restriction of the right to confidentiality of messages.⁸⁹ Transmission by a communications undertaking of messages to a central or portable surveillance device of a surveillance agency or security authority is decided by the surveillance agency or security authority. Electronic communications undertakings are required to keep information about surveillance activities and other data requests confidential.⁹⁰

Messages are transmitted to a central surveillance device using a splitting interface and appropriate hardware and software, which ensures the preservation of independent log files concerning the actions by means of the central surveillance device (time, type, object and number of action) for a period of five years. When the logs are destroyed, the electronic communications undertaking submits a detailed report to the supervisory authorities.⁹¹

For transmission of messages to a portable surveillance device, a surveillance agency or security authority sends an application in writing or by electronic means, which sets out the date, number and term of validity of the authorisation of a court for the conduct of a surveillance activity or for the restriction of the right to confidentiality of messages. The electronic communications undertaking preserves these applications for five years, after which time they should be destroyed and a report sent to the supervisory authorities.⁹²

While service providers' cooperation duties are broad and general under the CCP and the ECA, Estonian legislation does not provide the possibility to order service providers to break security measures or decrypt data. It needs to be pointed out that breaking security measures may entail covert entry into a computer system, and decryption of data may amount to wiretap, which are surveillance measures and are to be conducted by surveillance authorities. Service providers are not surveillance authorities; therefore, reliance on their assistance may render obtained evidence inadmissible, although it is also permitted to recruit persons for secret cooperation.

The lack of specific investigative measures or cooperation obligations of service providers have so far not caused significant obstacles in criminal investigations. The traditional and broad powers provided by the criminal procedural rules equip authorities with suitable tools to access and collect information when needed and most practitioners and commentators agree that the current legal framework is working well. Estonia is also a small country with relatively few local service providers, but with a tradition of stronger emphasis on informal relations. Service providers have been supportive in many respects and demonstrate commitment to cooperation with law enforcement in practice.

10.3.3 *Failure to Comply with Cooperation Requests*

The CCP provides that orders and demands by investigative agencies and the Prosecutor's Office in criminal proceedings are binding on everyone and allows for the pre-trial judge to impose fines on persons who have failed to perform such an obligation.⁹³ As follows from the discretion of the pre-trial judge, not every actual failure to comply will result in liability, but the CCP does not provide

⁸⁹ ECA Art. 113(1).

⁹⁰ ECA Art. 113(9).

⁹¹ ECA Art. 113(5).

⁹² ECA Art. 113(6).

⁹³ CCP Art. 215.

further details for service providers. Electronic communications undertakings can be held liable for violation of the obligation to preserve data and for violation of the obligation to provide information to surveillance agency or to grant access to communication networks under the ECA.⁹⁴

Failure to comply with requests has not been an issue at the domestic level and the cooperation generally works well. Nevertheless, some electronic communications undertakings check that formal requirements for demanding information are complied with by the requesting authorities and there have been cases where the service provider refused because it considered the request unlawful,⁹⁵ even if the legislation does not give service providers the power to assess the lawfulness of such requests. In any case, assessment by the service provider, or refusal to cooperate, does not, practically, extend to information provided by way of continuous electronic connection, since the latter implies ‘self-service’ by the authorities.

The sanctions for violation of the obligation to preserve subscriber and communications data are set out in Article 184¹ of the ECA; violation is punishable by a fine up to 300 fine units⁹⁶ or, in the case of legal persons, up to 3,200 euros. The same provision also covers violation of the obligation to preserve documentation (logs or applications) by electronic communication undertakings in relation to surveillance activities conducted by authorities. Pursuant to Article 185 of the ECA, violation of the obligation to provide information to surveillance agencies and the national security authority and to grant access to a communications network can incur a fine of up to 200 fine units, or up to 2,600 euros if committed by a legal person.

The CCP also provides for a general coercive measure, applicable to every case where the court or pre-trial judge has the right to impose a fine under the CCP, to ensure compliance with requests in criminal proceedings, and sets the amount at up to 3,200 euros (also repeatedly if necessary).⁹⁷ A fine imposed on a person for non-performance of an obligation does not release the person from performing the obligation.

10.3.4 *Use of Data Obtained from Service Providers: Admissibility and Complaints*

As explained in Section 10.2.1, strict evidence is used to prove facts related to the subjects of proof and free evidence can be used to prove the facts relating to a criminal case. If formal requirements are observed, data obtained through mandatory or voluntary cooperation can generally be used as evidence in court, with a few exceptions. Such exceptions concern cases where the evidence has been obtained by a criminal offence or in violation of a fundamental right.⁹⁸ However, the fact that evidence was not taken in accordance with the law does not automatically render evidence inadmissible in criminal proceedings in all cases. The only absolute prohibition on the use of evidence relates to cases where the requirements of law have not been complied with when applying for, or issuing, a permit for surveillance activities or performing such activities.⁹⁹ Courts have no discretionary power if requirements pertaining to surveillance activities have been violated and the resulting evidence is inadmissible.¹⁰⁰

⁹⁴ ECA Arts. 184¹ and 185.

⁹⁵ Chancellor of Justice, *Elektroonilise side seaduse § 111prim alusel sideandmete töötlemise põhiseaduspärasus* [Constitutionality of the Processing of Communications Data], 22 April 2016, No. 6-1/140621/1601788 para. 16.2, www.oiguskantsler.ee/sites/default/files/field_document2/elektroonilise_side_seaduse_ss_111_1_alusel_sideandmete_tootlemise_pohiseaduspärasus.pdf.

⁹⁶ Pursuant to Art. 47 of the PC, a fine unit is 4 euros.

⁹⁷ CCP Art. 138¹.

⁹⁸ CCP Art. 64(1).

⁹⁹ CCP 126¹(4).

¹⁰⁰ U. Lõhmus, *Põhiõigused kriminaalmenetluses* (Trükk: Juura, 2014), 81.

It is not prohibited to use evidence that has been taken in other proceedings. As an exception, the use of evidence collected by a person conducting other proceedings outside a criminal proceeding may not be permitted if the general conditions for gathering evidence provided for in Article 64 of the CCP or certain criminal procedural guarantees, such as the right not to be compelled to incriminate oneself, are not observed.¹⁰¹

Furthermore, information gathered through surveillance measures cannot be used as evidence in criminal proceedings if such information is covered by secrecy due to professional or other activity,¹⁰² such as client–attorney privilege or journalist source protection. However, this limitation is not absolute either and exceptions can be made, for example if the information at hand has already been disclosed or when the privilege is evidently misused.

The CCP sets out a notification obligation only for surveillance activities. After the expiry of the permission, the person with respect to whom the surveillance activities were conducted and the persons whose private or family lives were significantly violated by the surveillance activities and who were identified in the course of the proceedings are informed.¹⁰³ Hence, persons not participating in the criminal proceedings may also come to possess information about procedural activities, which can be subject to appeal and potentially affect the admissibility of evidence. Furthermore, service providers, which are obliged to cooperate with authorities in criminal investigations, do possess some information about procedural acts and material that is in the criminal file, to the extent that they have cooperated, but they are not entitled to request such information, unless they are the victim, a civil defendant, a suspect or a third party in the proceedings.

The CCP sets out the possibility of appeal against activities of investigative authorities and the Prosecutor’s Office, but persons entitled to do so may not even be aware of the use of their data in criminal proceedings. For instance, there is no specific notification obligation in the CCP with respect to the use of traffic and location data requested from electronic communications undertakings by investigative authorities, which essentially precludes exercise of the right of appeal. Moreover, complaints can be submitted only to protect one’s own rights; thus, service providers cannot challenge the admissibility of evidence on behalf of their customers.

Electronic communications undertakings inform their customers about the possibility of processing various categories of personal data, including traffic and location data, in their general privacy notices, or similar documents, as part of their duty to comply with the European Union’s General Data Protection Regulation (GDPR) (GDPR (EU) 2016/679 of the European Parliament and of the Council). Customers of service providers may submit information requests, including about to whom their personal data was disclosed, and responses from the service providers may reveal if traffic or location data requests were made by investigative authorities. In addition, information requests can be addressed to the investigative authorities themselves based on the Personal Data Protection Act (PDPA)¹⁰⁴ and thus potential violations of fundamental rights can be addressed. However, this needs a series of active steps by the data subject.

¹⁰¹ RKKKo 10 March 2012, 3-1-1-116-10, p. 8.

¹⁰² CCP Art. 126⁷(2).

¹⁰³ CCP Art. 126¹³.

¹⁰⁴ Isikuandmete kaitse seadus (Personal Data Protection Act), RT I, 4 January 2019, article 11, Arts. 37(4), 39(2) and 50(3).

10.3.5 Public Debates and Protection of Fundamental Rights

There are two main themes regarding digital evidence and the cooperation of service providers with law enforcement requests, as will be explained here. While both issues are interrelated, the most extensive discussion in media and academic publications pertains to mass data retention.

10.3.5.1 Distinction between Data Categories and Consequences Thereof

Various commentators,¹⁰⁵ including the dissenting judge in the *Onksion and others* case discussed in Section 10.2.5.2, have strongly criticised the distinction between content in transmission and content data at rest, as well as the distinction between content data and communication data. There are several problems with this approach. First, it is based on twentieth-century practice when an envelope could be clearly separated from its content. This is not the case anymore and traffic data may be revealing of the content (e.g., an internet protocol (IP) address can reveal what content was viewed by a person requesting data from a server). Second, technology has changed in that messages, in particular emails, are often stored on servers far away from recipients and hence it is questionable whether a user ever has the same level of control over his/her messages as was possible with regular mail. As the case of *Onksion and others* illustrated (see Section 10.2.5.2), the investigative authority could rely on its general powers under Articles 215(1) and 32 of the CCP to request production of emails from the service provider that was administering the private mail servers. Therefore, to the extent that the email is not stored locally on the recipient's device and/or in such a way that only the recipient has control over it, it remains disputable whether the level of control is the same as in the case of regular mail.

Despite some recent changes in the CCP, the Estonian understanding of the confidentiality of correspondence may still be contrary to both EU case law (see the *Digital Rights Ireland*,¹⁰⁶ *Tele2 Sverige*¹⁰⁷ and *La Quadrature du Net*¹⁰⁸ cases) and the interpretation of the European Convention on Human Rights¹⁰⁹ by the Strasbourg Court. Legislation distinguishes message content data from the related communication data, and the scope of the former is currently narrower than in the interpretation by the European Court of Human Rights, which held in *Malone* that records of metering, which corresponds to traffic and location data, are integral elements in the communication.¹¹⁰ This principle was extended to the internet in *Copland*.¹¹¹ The dominant position in Estonia, however, remains that data about a message can be separated from the content of the message itself. An absurd result of this distinction appears to be that, from the perspective of production orders and needed approvals, the content of a stored email enjoys less protection than the traffic and location data retained by electronic communications undertakings (i.e., a stored email, with its content, can be requested under the general powers by the prosecutor, while communications data requests are limited to serious crimes and need authorisation by a judge).

¹⁰⁵ U. Lõhmus, 'Veel kord õigusest sõnumite saladusele ehk kuidas 20. Sajandi tehnoloogia mõjutab põhiseaduse tõlgendusi' (2016) III *Juridica* 175–183.

¹⁰⁶ Case C-293/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others* and Case C-594/12, *Kärntner Landesregierung and others* [2014] ECLI:EU:C:2014:238.

¹⁰⁷ *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others*.

¹⁰⁸ Case C-511/18, *La Quadrature du Net and others v. Premier ministre* [2020] ECLI:EU:C:2020:791.

¹⁰⁹ Council of Europe, European Convention on Human Rights, ETS No. 005, 4 November 1950.

¹¹⁰ Application No. 8691/79, *Case of Malone v. The United Kingdom*, [1984] 7 ECHR 14, p. 84.

¹¹¹ Application No. 62617/00, *Case of Copland v. The United Kingdom*, [2007] 14 ECHR, pp. 43–44.

10.3.5.2 Mass Data Retention

Communication data can be used to fight serious crime, but how and under what conditions this data can be collected and for what purposes is a matter of controversy. Yearly there are about 3,000 permissions given to request retained data from electronic communications undertakings, which shows that this is an important measure in criminal investigations.¹¹² The Chancellor of Justice, who also serves as the ombudsman, found in her overview of 2019–2020 that communications data was requested and used in accordance with the law.¹¹³

Recent public debate relating to such data requests to electronic communications undertakings seems to focus on the security versus privacy dimension. However, this needs to be taken with a pinch of salt. It is also important to note the very high trust in the state among the local population and the low concern for violation of privacy when data is collected by the authorities. According to a 2020 survey on public perceptions concerning personal data protection, only 20 per cent of the survey respondents thought that the collection of data about people by the state is a threat to privacy and only 19 per cent found it very disturbing that the state can request their data from their internet service provider. Estonian residents consider collection of data by the state to be the safest – 66 per cent of the population believe that if the data collector is the state, then the data is also protected.¹¹⁴

The Estonian position on the CJEU's approach to data retention has always been critical. Karel Virks, Head of Bureau at the Estonian Internal Security Service, raised the question whether the e-Privacy Directive, which in the opinion of the CJEU regulates data retention in the member states, is merely establishing an exception and providing a sphere of autonomy for national regulation. Therefore, he argues, since the CJEU cancelled the Data Retention Directive, regulation of this area is within the competence of the member states.¹¹⁵ Also, all retained data is created in a business activity and in the context of provision of services; therefore, related risks (e.g., profiling of users) apply to such creation but not to the retention of the data.¹¹⁶

Against this backdrop, it does not come as a surprise that, following *Prokuratuur*, the Estonian media and some state officials publicly portrayed the consequences of the case as 'an obstacle to efficient investigations',¹¹⁷ with a few commentators even implying that the Supreme Court should be blamed for asking its questions of the European Court.¹¹⁸ In his response to the above positions, former Justice of the European Court of Human Rights Uno Lõhmus explained that the problem rather lies in that 'Estonia established and maintained the loosest personal data protection regime . . . and both the Riigikogu and law enforcement agencies hoped that we will continue to operate in the same way despite that our laws are in conflict with EU laws'.¹¹⁹

¹¹² Kriminaalmenetluse seadustiku muutmise seadus [Act Amending the CCP], 392 SE Seletuskiri, 20 December 2021, p. 4.

¹¹³ Õiguskantsleri aastaülevaade 2019/2020, Jälitustegevus, www.oiguskantsler.ee/ylevaade2020/jalitustegevus.

¹¹⁴ Kantar Emor, 'Inimeste privaatsusõigused ja /isikuandmete kaitsmine 2020', www.just.ee/media/494/download.

¹¹⁵ K. Virks, 'Sideandmed ja nende säilitamise olulisus' (2018) 8 *Juridica* 581–596.

¹¹⁶ *Ibid.*, 589–592.

¹¹⁷ T. Vahter, 'Suur sideandmete jama: Kelmid on nüüd kindlalt paremas seisus, nende tuvastamiseks peaaegu kõik võimalused läksid', *Eesti Ekspress*, 21 June 2021.

¹¹⁸ V. Voog, 'Riigikohus lasi sajad kohtuasjad õhku? Peaprokurör Parmas: tõendite kogumine võib osutuda võimatuks', *Õhtuleht*, 18 June 2021.

¹¹⁹ U. Lõhmus, 'Veelkord riigikohtu sideandmete otsusest ja selle käsitlusest meedias', ERR.ee, 25 June 2021 ('Eesti kehtestas ja säilitas kõige lõdvema isikuandmete kaitse režiimi. . . Ilmselt lootsid nii riigikogu kui ka õiguskaitseasutused, et meie seadused võivad küll olla vastuolus EL-i õigusega, kuid tegutseme vaikselt endisel moel edasi' (authors' translation)).

The esteemed judge previously also characterised the Estonian approach as that of a preventive state, which overestimates the risks and undervalues the fundamental freedoms.¹²⁰

Estonia consistently distinguishes aspects of collection and access within the data retention regime, and argues in favour of mass retention, while regulating conditions of access is a separate consideration. Minister of Justice Maris Lauri commented that although *Tele2* allows targeted retention, it would not only be very difficult and expensive but also lead to serious discrimination. Targeted retention could aim at the data of potential offenders based on profiling using personal traits, which is such a seriously discriminating activity that it certainly should not be done.¹²¹ She added that new CJEU judgments are expected to bring further clarifications regarding mass data retention and, when that happens, Estonia will take corresponding steps.¹²² Some called this approach the ‘Waiting for Godot’ mode.¹²³

Voices were also raised concerning the possibility of protecting privacy in the absence of knowledge about interference. Leading jurists have criticised the transparency of the current system, pointing out that ‘despite numerous requests, we were unable to access any logs that show who has accessed or used our phone data’.¹²⁴ However, it should be noted here also that this lack of transparency seems to concern the data processing practices of electronic communications undertakings, and Estonian residents (and e-residents¹²⁵) also have automated tools to check on how the authorities use their data that is in the state systems. Furthermore, they cannot be said to be unaware of the possibility of data requests being made in relation to them in criminal investigations, since the laws publicly state this, and it is practice by all major electronic communications service providers to inform their clients about such data processing purposes.

Notification can be received in the context of surveillance activities according to Article 126¹³ of the CCP, which provides that at the expiry of the authorisation the surveillance agency shall immediately notify the person with respect to whom the surveillance activities were conducted and the person whose private or family life was significantly violated by the surveillance activities and who was identified during the proceedings. However, exceptions can be made.¹²⁶ Given that retained traffic and location data are processed according to the above Estonian legal framework that still relies on mass data retention, the fact that proactive notification requirements, like those under the surveillance measures, are lacking in the relevant articles of the CCP remains a concern.

In addition, Estonian legislation provides for continuous connection to communications undertakings’ networks for the purposes of accessing retained communications data without making a separate request. Yet, current regulation does not require to provide statistical data about such uses; there is no regulation on keeping or destroying relevant log files; and it is unclear whether the state has a full overview about the use of such direct access. However, it can be presumed that when the authority can have direct access to the data, it is deemed necessary and there is no need to go through the whole bureaucratic process of requesting such data from communications undertakings. Cooperation is then functional and appears to be automated to a great extent, due to ‘continuous electronic connections’ that imply self-service for investigating

¹²⁰ U. Lõhmus, ‘Jälgimine ja põhiõigused’ (2020) 4 *Juridica* 279.

¹²¹ M. Lauri, ‘Maris Lauri: sideandmetest nii ja naa’, ERR.ee, 24 September 2021.

¹²² Ibid.

¹²³ C. Ginter, ‘Carri Ginter: ametnikud tõmbavad riigikogule “mütsi pähe”’, ERR.ee, 10 September 2021.

¹²⁴ Ibid.

¹²⁵ E-residency is a government-issued digital identity and status for non-residents/non-citizens that provides access to Estonia’s e-government services and business environment. See, e.g., www.e-resident.gov.ee/.

¹²⁶ CCP Art. 126¹³.

bodies, to some extent at least. Yet, there is virtually no transparency about how these connections function.

Although the current legal framework has weaknesses in safeguarding the fundamental rights of data subjects related to criminal proceedings, the problems arising from such gaps may be offset by the trust and high expectations of the local population towards the e-state, which has so far demonstrated attention, prudence and responsibility in addressing the security risks inherent in dependence on ICT. Respect by the authorities towards the people is well illustrated by Estonia's ranking second place on the freedom of the internet list in 2021¹²⁷ and fifteenth on the freedom of expression index;¹²⁸ it is a consolidated democracy with a percentage indicator of 84/100¹²⁹ and ranks the third most secure country on the Global Cybersecurity Index.¹³⁰ Population sentiment can support the argument that the Estonian authorities are exercising their margin of appreciation (i.e., the space for manoeuvre) in fulfilling their obligations arising from human rights instruments. On the other hand, one can also entertain the argument that the above data reflects low general awareness about privacy and fundamental rights among the Estonian population.

Carrying out digital investigations is an exercise that puts things into a different perspective. Yet, one needs to be conscious that one of the foundations of a successful digital state is the trust of the people, which has been apparently earned by savvy solutions and transparency so far. Therefore, it is imperative that the pieces of necessary checks and balances fall in their right places regarding rule of law and protection of fundamental rights.

10.3.6 *Personal Data Protection Act (PDPA)*

As noted earlier, a body conducting criminal proceedings has the right to process personal data, including special categories of personal data, which are required for conducting pre-court proceedings and judicial proceedings, gathering evidence, enforcement of the decisions made in criminal matters, performing surveillance activities or achievement of other objectives provided for in the CCP.¹³¹ The body conducting criminal proceedings shall act as a LEA when processing personal data and the processing of such data shall be guided by the provisions established for LEAs.¹³²

The PDPA implements the provisions of the Law Enforcement Directive (LED),¹³³ which governs personal data protection rules in the context of criminal proceedings. According to Article 13(2) of the PDPA, LEAs are deemed to include any agencies or structural entities of agencies which are competent pursuant to law to prevent, detect and prosecute offences and execute punishments. Though the rules stipulated in the PDPA have direct effect in the

¹²⁷ Freedom on the Net report, Freedom House, freedomhouse.org/countries/freedom-net/scores?sort=desc&order=Total%20Score%20and%20Status.

¹²⁸ S. Hankewitz, 'Estonia Drops a Place in the 2021 World Press Freedom Index', *Estonian World*, 22 April 2021.

¹²⁹ L. Taving, 'Estonia: Nations in Transit 2021', Freedom House, 2021, freedomhouse.org/country/estonia/nations-transit/2021.

¹³⁰ e-Estonia, 'Estonia Ranks as the Third Most Secure Country on the Global Cybersecurity Index', 1 July 2021, e-estonia.com/estonia-the-3rd-most-secure-country/#:~:text=In%20the%20Global%20Cybersecurity%20Index,is%20the%20most%20secure%20country.

¹³¹ PDPA Art. 15.

¹³² PDPA Art. 15.

¹³³ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, [2016] OJ L 119, 4 May 2016.

processing of personal data, these rules are not absolute and shall not apply to the state and administrative supervision.¹³⁴ Chapter 4 of the PDPA applies to processing of personal data by LEAs to the extent that they perform activities in their function of preventing, detecting and proceedings of offences and execution of punishments.¹³⁵

Given that collection of digital evidence is required for the prevention, detection and prosecuting of offences and the execution of punishments and therefore assumes processing of a large amount of data, including when necessary special categories of personal data, the principles of processing personal data in the PDPA are in accordance with the principles of processing personal data enshrined in Article 5 of the EU's GDPR.¹³⁶ These principles include legality and fairness, purposefulness, quality, accuracy, retention and security.¹³⁷ These principles must also be followed when personal data have to be transmitted to recipients in any third country for the purposes of prevention, detection and proceedings of offences or execution of punishments by law enforcement agencies.¹³⁸ Given that time is a crucial and decisive element in criminal proceedings, one may argue that automatic processing of personal data, including profiling, should be allowed in criminal matters as part of collecting digital evidence. However, Article 21 of the PDPA – in line with Article 11 of the LED – prohibits decision-making based solely on automated processing, including profiling, to avoid adverse legal consequences for the data subject or discrimination of natural persons.

In general, in criminal proceedings, rights of data subjects are guided by the provisions laid down in the CCP, regardless of whether the data subject is a suspected, accused, victim, civil defendant, third party, witness or any other person. Nevertheless, the rights of data subjects that can be restricted, in cases prescribed by law, during criminal proceedings include: the right to know that their personal data are processed, including what personal data are processed, and the way, method, objective, legal basis, extent or cause of the processing; the right to know the recipients of their personal data and the categories of personal data disclosed and information about whether their personal data is transmitted to foreign countries or international organisations; the right to demand restrictions on processing of their personal data; the right to object to processing of their personal data; and the right to know about breaches related to their personal data.¹³⁹ In accordance with Article 13(3) of the LED, such exceptions apply in cases where the restriction is necessary for prevention, detection or proceedings of offences or execution of punishments; to protect the rights and freedoms of other persons; for the purposes of national security; for protection of the public order; or to avoid hindering formal investigations or proceedings.¹⁴⁰ Furthermore, processing of personal data, including special categories of personal data, is allowed for the purposes of identifying the background check of a person.¹⁴¹

To process data in compliance with the rules and principles established in the PDPA, LEAs must designate data protection specialists. Subsequently, courts are released from this obligation upon performance of the function of administration of justice.¹⁴²

¹³⁴ PDPA Art. 12(3).

¹³⁵ PDPA Art. 12(1).

¹³⁶ Regulation (EU) 2016/679 of 27 April 2016.

¹³⁷ PDPA Art. 14.

¹³⁸ PDPA Art. 49.

¹³⁹ PDPA Arts. 23–24.

¹⁴⁰ PDPA Art. 23(2).

¹⁴¹ Politsei ja Piirivalve Seadus (Police and Border Guard Act), RT I 2009, 26, 159; RT I, 27.05.2022, 28. In force since 1 July 2022, Art. 7⁵⁹.

¹⁴² PDPA Art. 40.

10.4 CROSS-BORDER COOPERATION BETWEEN LEAs AND SERVICE PROVIDERS

10.4.1 *Overview and Principles*

Estonia is a small country and relies heavily on foreign services and service providers for the functioning of its information society. It would be difficult to demonstrate by precise numbers what is the proportion of investigations with some foreign element, since the understanding is that access to data in Estonia confers jurisdiction to collect it and it is then hard to distinguish cases which are purely domestic in all respects. Therefore, Estonia has a broad interpretation of jurisdiction, and claiming jurisdiction would not be a hindrance in criminal proceedings.

Furthermore, Article 65 of the CCP foresees that the evidence taken in a foreign state pursuant to the legislation of such state may be used in criminal proceedings conducted in Estonia unless the procedural acts performed to obtain the evidence conflict with the principles of Estonian criminal procedure, and so far it covers evidence from a foreign state by way of a request for legal assistance.

Cases where there is a need to collect digital evidence from another state, or when the location of the data is unknown ('loss of location'), constitute so far unregulated situations as there are no special provisions in the CCP to this effect,¹⁴³ and the courts have not voiced any opinion regarding 'internet jurisdiction'. Nevertheless, cooperation between law enforcement and foreign service providers is everyday practice and evidence is being collected from foreign servers in criminal investigations.

The case of *Onksion and others* (see Section 10.2.5.2), however, may shed some light on this issue, but more from the perspective of what was *not* addressed by the Supreme Court. The Court held that accessing stored data, such as unread emails in a Gmail inbox from the territory of Estonia, is not wiretapping but covert examination of a thing, that is, covert search.¹⁴⁴ Curiously, in this case, the Court did not find it necessary to consider questions of jurisdiction, as if covertly searching a server located in a foreign state by remote connection would not require further consideration.¹⁴⁵ It is not possible to explain this missing piece in the decision by irrelevance of the matter. It is more likely that leaving the question of jurisdiction out of the legal analysis was a very conscious choice of the judges. Considering the potential consequences of any ruling or opinion on this matter by the court, they would have opened 'Pandora's box' and created more problems than they solved.

This interpretation of the Supreme Court's case law may also shed light on the question why there are no planned rules on remote searches in the proposed amendments to the CCP¹⁴⁶ in the overall reform. If the system of rules governing criminal procedure works well in practice, it is sufficient to make minor improvements, but it may be counterproductive to touch on an issue that could lead to serious restriction of Estonian law enforcement powers.

Traditional territoriality criteria, such as location of data, service provider or data subject, carry little relevance in collecting digital evidence by LEAs in Estonia. Other states are also increasingly adopting alternative approaches¹⁴⁷ (e.g., jurisdiction based on access, control and

¹⁴³ A.-M. Osula, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (2016) 24(4) *International Journal of Law and Information Technology* 343–373.

¹⁴⁴ RKKKo 20 November 2015.

¹⁴⁵ Lõhmus, 'Põhiõigused kriminaalmenetluses', 360.

¹⁴⁶ *Explanatory Note to the Draft Law Amending the Code of Criminal Procedure and Other Laws (Revision of Code of Criminal Procedure)*, 1.

¹⁴⁷ For example, the United States' Clarifying Lawful Overseas Use of Data (CLOUD) Act of 23 March 2018.

possession of data, rather than location of data); hence, a similar practice is followed in Estonia.¹⁴⁸ For instance, it interprets its laws so as to give effect to Article 32 of the Cybercrime Convention. Law enforcement can access, without the authorisation of another state, publicly available (open source) stored computer data, regardless of where the data is located geographically; Estonian authorities do access and receive through computer systems located in Estonia stored computer data located in foreign servers. Authority to give consent can be interpreted in the light of the jurisdictional rules of Estonia; hence, consent can be obtained from the data subject (for instance, voluntary disclosure of usernames and passwords) or from the Estonian courts, which have the right to authorise the collection of data that can be accessed in the territory of Estonia. Admittedly, this approach is not without controversies, and perhaps this is the reason why Estonia chooses not to stir the calm waters with public statements or legislative action on how it implements Article 32.

Thus, no request for legal assistance is necessary for observing or collecting data stored in the cloud or foreign servers, provided that the investigative measures set forth in the CCP are used. With these tools, Estonian law enforcement can effectively eliminate the need to resort to mutual legal assistance treaties (MLATs) in most cases. Also, for the purposes of collecting information for use in criminal proceedings, but not for use as evidence in court, fewer formalities apply. For instance, there is no need to comply with the formal requirements of strict evidence and thus MLAT requests may not be necessary at all.

However, this applies only to data, and the fact that a service is available in the territory of Estonia does not confer jurisdiction for purposes of criminal investigations. Hence, depending on the case at hand, if Estonian LEAs cannot get the necessary information themselves, they have no other choice but to rely on either informal cooperation with foreign service providers or mutual legal assistance frameworks. It is decided by external factors when LEAs resort to existing legal cooperation frameworks and mediated cooperation with foreign service providers where appropriate.

The CCP was amended in 2017¹⁴⁹ to implement the European Investigation Order (EIO) Directive.¹⁵⁰ Although the implementation did not generate virtually any discussion relating to digital evidence, the EIO Directive is welcome as it is expected to speed up response to Estonian cooperation requests, although the speed of Estonian responses may be affected due to stricter requirements.¹⁵¹ Estonian law enforcement is in general satisfied with the EIO Directive, and any questions concern practices to increase the effectiveness of existing mechanisms, in particular the speed of answers.

The effects of the implementation of the LED cannot be neglected either. While Estonian LEAs rely heavily on cooperation with US service providers and information obtained from foreign servers, the new rules of the PDPA impose some restrictions on cooperation with foreign authorities. Article 4 of the PDPA refers to the GDPR and essentially requires that the recipient

¹⁴⁸ A.-M. Osula, 'Täidesaatev jurisdiktsioon ja piiritlene kaugläbiotsimine' (2017) 8 *Juridica* 564.

¹⁴⁹ Kriminaalmenetluse seadustiku ja kriminaalmenetluse seadustiku rakendamise seaduse muutmise seadus (Euroopa uurimismääruse direktiivi ülevõtmine) [Act Amending the Code of Criminal Procedure Act and the Implementation Act of the Code of Criminal Procedure (Transposition of the European Investigation Order Directive)], RT I, 26.06. 2017, 70. In force since 6 July 2017.

¹⁵⁰ Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, [2014] OJ L 130, 1 May 2014.

¹⁵¹ Minutes of Meeting No. 121 of the Parliament's Legal Commission of 8 May 2017. Urmas Reinsalu's (then Minister of Justice) explanation to a question of Valdo Randpere (MEP): 'Does the transposition of the EIO Directive change the principles of our criminal procedure?'; Answer: 'No, ... but we will have the obligation to provide assistance to other states in a more rigid manner' (authors' translation).

state guarantees an adequate level of personal data protection. This can be assessed by the existence of adequacy decision of the European Commission or lack thereof; or by individual assessment of the appropriateness of safeguards provided in the legislation of the foreign state; or if the recipient, taking into account all circumstances relating to the transfer of personal data, has applied all appropriate measures to protect personal information.¹⁵² Exceptions pursuant to Article 48 of the PDPA allow transfer of personal data for the purposes of protection of the rights and freedoms of the data subjects or any other persons, to safeguard legitimate interests of the data subjects, for the prevention of an immediate and serious threat to public security, and in individual cases for establishment, exercise or defence of legal claims relating to the purposes of prevention, detection, prosecution of criminal offences or execution of criminal penalties. These provisions are designed to prevent the frequent, extensive, structured or mass transfer of personal data and should not affect cooperation between countries if it done on a case-by-case basis.¹⁵³

10.4.2 Cooperation between Estonian LEA and Foreign Service Providers

Foreign service providers are used heavily in the Estonian information society. This is no surprise since the approximately 1.5 million inhabitants of the country do not provide a rich market for locally oriented social media, email services or other platforms. Estonians are rather outward-looking in this respect and often rely on foreign service providers, at least parallel to local ones. As a result of this attitude, criminal investigations have needed to adapt and seek information from the most often used platforms and providers, such as Facebook and Google.

According to transparency reports, Estonia has made fifty-eight requests to Facebook and in 43 per cent of those cases the company produced some data in the second half of 2021.¹⁵⁴ Google reported ninety-one user data disclosure requests from Estonia in the second half of 2020, and produced some data in 86 per cent of the cases.¹⁵⁵ Seven requests went to Microsoft in the second half of 2021, two of which resulted in non-content data disclosure; the rest were rejected or data was not found.¹⁵⁶

There are no powers in the CCP to oblige foreign service providers to comply with Estonian orders and direct cooperation between Estonian LEAs and foreign service providers takes place on a voluntary basis. Since the cooperation between Estonian LEAs and foreign service providers is not regulated in Estonian legislation – and can thus be considered ‘informal cooperation’ – investigators simply need to follow the conditions set by these providers. No concerns were raised in this respect in recent years; in fact, both the courts and the executive have rather avoided these questions.

In addition, if the domestic rules on gathering evidence are observed (which are rather flexible), there are no issues on the admissibility of evidence obtained based on informal cooperation with foreign service providers, and, to our knowledge, no questions in this respect have so far been raised. The use of information obtained through voluntary or informal cooperation is not precluded as such by the CCP.

Estonia has consistently participated in the preparation of and welcomes the new rules of the Second Additional Protocol to the Cybercrime Convention.¹⁵⁷ Although cooperation with

¹⁵² PDPA Art. 47.

¹⁵³ Transposition of the European Investigation Order Directive, Explanatory memorandum (*seletuskiri*), p. 42.

¹⁵⁴ Facebook, Facebook Transparency Report, transparency.fb.com/data/.

¹⁵⁵ Google, Google Transparency Report, transparencyreport.google.com/?hl=en.

¹⁵⁶ Microsoft, Microsoft Transparency Overview, www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report.

¹⁵⁷ P. Paukštyš, ‘Rahvusvaheline koostöö küberkuritegude uurimisel’, Prokuratuuri Aastaraamat, 2021.

foreign service providers works well, these informal frameworks have their limitations and law enforcement cooperates with foreign service providers to the extent to which it is allowed by the laws of the service provider's state. This does not guarantee that all requests will be answered, and in practice LEAs sometimes receive the requested information and sometimes they do not. Furthermore, not all types of data can be requested under the voluntary mechanisms.

Estonia is no exception, and thus when content data is needed, Estonian LEAs need to launch official procedures and use mutual legal assistance frameworks. In 2020 Estonia sent out 414 mutual legal assistance requests and European Investigation Orders (EIOs) and received 1,166.¹⁵⁸ The above-mentioned Second Additional Protocol is expected to somewhat increase the effectiveness of the cooperation and investigative measures by allowing direct requests to foreign service providers and deadlines for responding.¹⁵⁹

10.4.3 *Cooperation of National Service Providers with Foreign LEAs*

Article 156 of the Penal Code (PC) protects confidentiality of messages communicated by letter or other means of communication. Also, illegal disclosure of personal data, if it is obtained during professional activities by a person who is required by law not to disclose such information, is an offence pursuant to Article 157 of the PC. Article 157¹ deals with illegal disclosure of sensitive personal data.

According to Article 102 of the ECA, a communications undertaking is required to maintain the confidentiality of all information which becomes known to it in the process of its provision of communications services and which concerns subscribers as well as other persons. It must maintain the confidentiality of:

- (1) information concerning specific details related to the use of communications services;
- (2) the content and format of messages transmitted over the communications network;
- (3) information concerning the time and manner of transmission of messages.

The ECA lists the authorities to which information is provided upon request. Foreign authorities are not included in the list; hence, direct cooperation with foreign LEAs is effectively precluded by Estonian legislation, unless the request concerns non-personal data that is considered to be stored non-content data (e.g., certain financial data, as well as certain technical or sensor data and so on). The authors are not aware of any potential or actual cooperation between national service providers and foreign LEAs, although one may point out the need for reciprocity.

10.4.4 *Opportunities and Challenges Created by the e-Evidence Regulation*

The general objective of the recently adopted e-Evidence Regulation is to ensure effective investigation and prosecution of crimes in the EU by improving cross-border access to electronic evidence through enhanced judicial cooperation in criminal matters and an approximation of rules and procedures.¹⁶⁰ This Regulation is not expected to require many changes in Estonian legislation.

¹⁵⁸ Ibid.

¹⁵⁹ E. Rattam, 'Pilves selgimistega tulevik ehk mõningatest rahvusvahelise küberkuritegevuse tõkestamise väljakutsetest digitaalsete tõendite kogumise kontekstis', Prokuratuuri Aastaraamat, 2021.

¹⁶⁰ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191/118, Recitals 2-9 (e-Evidence Regulation).

The new Regulation provides for direct cross-border cooperation with foreign service providers, aiming for the production or the preservation of data. At present, the cross-border collection of data is already possible using the EIO Directive; yet, the new procedure will be different. While execution of an EIO necessarily requires cooperation between the issuing and the executing authority, a European production order under the e-Evidence Regulation in principle does not involve the implication of the enforcing authority, unless the service provider refuses to execute the order. Moreover, with an EIO, it is ensured that the execution shall be in the same way and under the same modalities as if the investigative measure concerned had been ordered by an authority of the executing state. When asking the same kind of information through a European Production Order, only the rules of the issuing member state will apply, with some exceptions, for instance for immunities and privileges.¹⁶¹ The coexistence of two instruments for cross-border cooperation may result in overlaps and cause confusion in practice, especially considering that Estonia does not have a distinct category for digital or electronic evidence. Furthermore, given that all formal procedural rules are enacted for prolonged periods and are time-consuming, the aim of having dedicated platforms or other secure channels for the handling of requests for data by law enforcement and judicial authorities is crucial in this matter. The importance of creating a decentralised IT system can thus not be overestimated.¹⁶²

Furthermore, the new e-Evidence Regulation will bring changes in respect of the grounds that service providers can invoke for refusal to cooperate. De facto, the impossibility of complying with requests of LEAs can be solved reasonably under current legislation (see Section 10.3.3). That said, any clarification on the procedure and conditions to invoke these grounds would bring more clarity to existing rules. In a case where the order ‘contains manifest errors or does not contain sufficient information to execute’ it, the service provider should inform the issuing authority ‘without undue delay’ and seek clarification, thus entering into a constructive dialogue with the issuing authority.¹⁶³

10.5 CONCLUSION

Estonia is undoubtedly an e-state. The legislative framework governing digital evidence has been analysed in the ongoing criminal law reform aimed at transitioning to fully digital criminal proceedings. The proposed changes to the CCP reflect the understanding that the current broad and general powers set out in the CCP are practical and appropriate tools for effective investigations, and instead of extensive changes, only relatively minor adjustments and clarifications are needed concerning digital evidence. Estonian LEAs rely on traditional investigative measures to gather digital evidence and only a few specific provisions are provided for requesting subscriber data and transaction data from service providers; somewhat more detailed rules govern the application of covert measures. Cooperation between (the relatively few) domestic service providers and law enforcement has been good throughout the years. The CCP and the ECA regulate the cooperation duties of electronic communications undertakings, including mobile operators and internet service providers.

While the legal regime governing digital evidence and cooperation between law enforcement and service providers has its own flaws, no major criticism can be identified as to the entire system. More transparency would always be welcome, but the greatest problem may lie in the distinction between messages in transmission and recorded (or stored) messages. However, any

¹⁶¹ See, e.g., E-Evidence Regulation, Arts. 10(5) and 11(4).

¹⁶² Ibid., Ch. V.

¹⁶³ Ibid., Art. 10(6).

changes in this respect would need either a change of the Constitution or the Supreme Court to reverse its position regarding this interpretation – both of which require serious changes in the circumstances and general attitudes relating to the issue, and the idea of any change does not currently seem to be gaining traction with the legislator or the courts.

The Estonian CCP and ECA have been strongly influenced by European case law and now, with the signature of the Second Additional Protocol to the Cybercrime Convention on 12 May 2022, it is expected that it will bring some new changes in the legislation. These external factors seem to be driving the adaptation of the rules domestically. However, it should also be stressed that not all these influences are received with much enthusiasm, and especially the CJEU's data retention jurisprudence is regarded with scepticism and minimalistic solutions are sought for implementing the Court's rulings. On the other hand, new EU and international legislation that aims to ease and improve the procedures in digital investigations is generally welcome as it confirms Estonia's already existing practices and their effectiveness.

The size of the country is, obviously, a determining factor for the outward-looking nature of criminal investigations. Estonian law enforcement relies heavily on information obtained from foreign servers, yet there is very little in the law that addresses this issue. The need to reach beyond the borders of this small country is supported by the permissive interpretation of the jurisdictional rules. Estonian law enforcement and courts tacitly accept this approach and consider that jurisdiction to collect data is conferred by the fact that data is accessible in the territory of Estonia. Hence, data copying also takes place in Estonian territory by authorised officials without leaving the country. Until now, no serious obstacles have been encountered in this approach; however, Estonia does not go as far as to impose obligations on foreign service providers by virtue of them providing their services in Estonia. Cooperation with foreign service providers takes place on the same basis as they cooperate with other countries. Estonian LEAs follow the instructions given and their requirements, and often receive a response. Estonia has also welcomed the EIO Directive, and the only main criticism is that cooperation could be even faster – a concern that will be addressed by the e-Evidence Regulation.

Overall, Estonia's motto could be presented as: 'If it isn't broke, don't fix it.' However, regardless of the approach taken, ensuring fundamental rights should be a priority.

Digital Evidence and the Cooperation of Service Providers in Germany

*Dominik Brodowski**

11.1 SETTING THE SCENE

In a strict sense, German criminal procedure does not know of ‘digital evidence’. In Germany, only specific means of ‘evidence’ may be introduced in a criminal trial to prove the guilt of the accused, namely – besides statements by the accused – only inspection, that is, the sensory perception of evidence (*Inaugenscheinnahme*), documentary evidence (*Urkundsbeweis*), witnesses (*Zeugenbeweis*) and expert statements (*Sachverständigenbeweis*).¹ As digital data – such as is stored in a file on a flash drive – cannot be perceived sensorially or directly read by humans, it cannot be introduced into a criminal trial as ‘evidence’ itself. Instead, any digital data first requires some transformation into ‘evidence’ which may then be introduced in trial.² For example, a text document may be processed by the usual software, printed out and then read as a document; a video may be shown on a screen and then perceived visually; or a complex business calculation in a spreadsheet may be assessed by an expert who is then called as a witness. Based on such a strict understanding, data cannot be ‘evidence’ in a legal sense; instead, the focus is on ‘digital traces’ – that is ‘traces, based on data, which are stored or transferred in computer systems’³ – which require further analysis, interpretation and transformation to be available as ‘evidence’ in court.⁴ In a broader sense, however, ‘digital evidence’ may be used as the term for any digital traces which are to be used in furtherance of a criminal investigation.⁵ This is the approach taken in the subsequent analysis – yet it should always be kept in mind that, owing to the need of interpretation and transformation, ‘digital evidence’ is easy to be misperceived as ‘objective’, ‘reliable’ and ‘convincing’.⁶

* The author thanks Dr Nicolas von zur Mühlen for his extensive preliminary research conducted in furtherance of this chapter.

¹ See Michael Bohlander, *Principles of German Criminal Procedure*, 2nd ed. (Oxford: Hart, 2021), 146–163.

² Dennis Heinson, *IT-Forensik* (Tübingen: Mohr Siebeck, 2015), 106–123; Matthias Jahn and Dominik Brodowski, ‘Digitale Beweismittel in strafprozessualer Hauptverhandlung und Revision’, in Bernd Hecker, Bettina Weißer and Christian Brand (eds.), *Festschrift für Rudolf Rengier zum 70. Geburtstag* (Munich: C. H. Beck, 2018), 409–412 with further references.

³ Andreas Dewald and Felix Freiling, *Forensische Informatik*, 2nd ed. (Norderstedt: BoD, 2015), 29 (author’s own translation).

⁴ Heinson, ‘IT-Forensik’, 122; Jahn and Brodowski, ‘Digitale Beweismittel’, 409–412.

⁵ See already Jahn and Brodowski, ‘Digitale Beweismittel’, 409 in fn. 5.

⁶ On this fallacy, see Carsten Momsen, ‘Zum Umgang mit digitalen Beweismitteln im Strafprozess’, in Christian Fahl, Eckhart Müller, Helmut Satzger and Sabine Swoboda (eds.), *Ein menschengerechtes Strafrecht als Lebensaufgabe. Festschrift für Werner Beulke zum 70. Geburtstag* (Heidelberg: C. F. Müller, 2015), 875–884; Jahn and Brodowski, ‘Digitale Beweismittel’, 414–415.

11.1.1 General Approach to the Collection of Digital Evidence

11.1.1.1 Collecting Physical Evidence: Extension and Modification of Digital Evidence

The primary approach to collecting digital evidence in Germany is to search for (§§ 102 ff. German Code of Criminal Procedure (*Strafprozessordnung* – *StPO*))⁷ and seize (§§ 94 ff. *StPO*) data storage devices, ranging from tiny flash drives to large-scale server systems, as physical evidence.⁸ That approach builds upon the pre-existing provisions in the German Code of Criminal Procedure governing these measures, and makes use of the fact that unless data is transmitted, it does not exist ‘in the air’, but requires physical devices for storage and procession. In addition to seizing an object by force, authorities have the power to demand that the specific object of interest for the criminal investigation is handed over to the authorities by those who have it in their possession (production order, § 95 [1] *StPO*, see further Section 11.3.3.1) – unless they are suspects or accused, as those cannot be legally forced to actively participate in a criminal investigation against themselves, based on the constitutional ground of *nemo tenetur se ipsum accusare*. Yet, they can still be granted the opportunity to hand over the objects of interest themselves, and thereby avert that the authorities search and seize these objects by force.

A search of premises, a subsequent seizure of objects which are relevant for a criminal investigation and a production order require a specific, ongoing criminal investigation of a concrete (past or ongoing) criminal offence.⁹ The search of premises is generally subject to *ex ante* judicial review (§ 105 *StPO*), while seizure and production orders are subject – at least upon request by an affected party – to *ex post* judicial review (§ 98 *StPO*). Limitations stem, in particular, implicitly from a proportionality requirement and explicitly from protections of professional privileges such as the client–attorney privilege (§ 97 *StPO*).¹⁰ A *maiores ad minus*, it is well accepted that not only physical devices can be seized by authorities or requested by a production order but also electronic data as such – in particular, by making a copy of it.¹¹

Notably, although more specific provisions (see Section 11.1.1.3) prevail under the *lex specialis* rule, there is no explicit limitation on what types of data can be collected by searching for and seizing a data storage device, by seizing data or by requiring its production. For instance, it is well accepted that data stemming from *past* telecommunication, such as a chat message on a suspect’s computer, can be obtained by such means (compare with §§ 100g [5], 100 k [5] *StPO*). According to a decision of the German Federal Constitutional Court, even data relating to *ongoing* telecommunication that is stored with a service provider can be obtained based on these provisions.¹²

⁷ Strafprozessordnung of 1 February 1877 (German Code of Criminal Procedure), *Reichsgesetzblatt (RGBl.)* 1877, 253, as amended. An unofficial and partially outdated translation provided by the German Ministry of Justice is available at www.gesetze-im-internet.de/englisch_stpo/.

⁸ See Ulrich Sieber and Dominik Brodowski, ‘19.3 Strafprozessrecht’, in Thomas Hoeren, Ulrich Sieber and Bernd Holznapel (eds.), *Handbuch Multimedia-Recht*, 60th ed. (Munich: C. H. Beck, 2024), margin number (mn.) 50, 65.

⁹ German police laws, which focus on how police may avert dangers – including dangers stemming from criminal offences up to terrorism – also include legal bases for collecting information. See Dominik Brodowski, ‘Alternative Enforcement Mechanisms in Germany’, in Matthew Dyson and Benjamin Vogel (eds.), *The Limits of Criminal Law* (Cambridge: Intersentia, 2018), 385–387; Marc Engelhart, ‘Countering Terrorism at the Limits of Criminal Liability in Germany’, in Matthew Dyson and Benjamin Vogel (eds.), *The Limits of Criminal Law* (Cambridge: Intersentia, 2018), 435–466.

¹⁰ For an overview, see Bohlander, ‘German Criminal Procedure’, 83–87.

¹¹ Bundesverfassungsgericht (German Federal Constitutional Court), Order of 12 April 2005, 2 BvR 1027/02; German Federal Constitutional Court, Order of 18 February 2003, 2 BvR 372/01.

¹² German Federal Constitutional Court, Order of 6 June 2009, 2 BvR 902/16.

Traditionally, these measures of search and seizure as well as production orders are governed by a regime of transparency and openness, also towards the suspects and accused. Several court decisions highlighted the need to readily inform suspects of a seizure of their data (such as their email accounts), even if the data was seized from a third party, such as their email provider. Furthermore, the German Federal Court of Justice held, based on the proportionality principle, that this information must be provided to suspects early enough so that they can assist in filtering out the relevant data.¹³

In 2021, however, the German Code of Criminal Procedure was amended¹⁴ to allow for a delayed notification of suspects (§ 95a [1] StPO) in case the production order or the search and seizure relates to an object (or data) not in their possession; those who had the object in their possession may concurrently receive a ‘non-disclosure order’ (§ 95a [6] StPO) prohibiting them from informing the suspect of the measure. Although limited materially to offences of a substantial significance (including but not limited to those listed in § 100a [2] StPO) as well as procedurally (by a requirement of judicial authorisation), this provision is being heavily criticised for undermining the specific, more limited provisions governing clandestine surveillance measures (§§ 100a ff. StPO) in violation of constitutional guarantees.¹⁵ Moreover, it is unclear whether these provisions actually apply to the common and intended purpose of secretly obtaining emails or chat messages stored with a service provider: it can well be argued that such data is not in sole possession of the service provider but also in the possession of the user, making § 95a StPO unavailable.¹⁶

Oftentimes, when storage devices or (raw) data are obtained, these are encrypted and/or require in-depth forensic analysis. Generally speaking, the German Code of Criminal Procedure does not contain an explicit legal basis for the analysis of data, in particular if that would require circumventing encryption. While some argue that such an analysis of ‘evidence’ obtained by the authorities is generally legal,¹⁷ others point to the intrusion into privacy which follows from, for example, breaking into a mobile phone, and call for a more restrictive legal basis.¹⁸ At least it is clear since an amendment enacted in 2021¹⁹ that (raw) data preliminarily obtained during a search of premises (§§ 102 ff. StPO) may be sifted through first, before deciding on the formal seizure of a storage device or data (§ 110 [3] 1 StPO).

11.1.1.2 ‘Remote Searches’ for Digital Evidence

Addressing the volatility and transferability of data, the German legislature introduced a provision in 2009 to allow authorities, during the searching of a premise, to extend their search to ‘physically separate storage media’ – that is, storage media located in remote locations – insofar as such media is accessible from a storage medium found during the search of the

¹³ Bundesgerichtshof (German Federal Court of Justice), Order of 4 August 2015, 3 StR 162/15; German Federal Court of Justice, Order of 26 January 2017, StB 26/14, StB 28/14.

¹⁴ Bundesgesetzblatt (BGBl.) 2021 I, 2099.

¹⁵ See Mayeul Hiéramente, ‘Heimliche Handlungen – zur geplanten Einführung einer heimlichen Beschlagnahme’ (2021) 3 *juris PraxisReport Strafrecht* 1.

¹⁶ Dominik Brodowski, ‘§ 95a StPO’, in Georg Borges and Marc Hilber (eds.), *Beck’scher Online-Kommentar IT-Recht*, 14th ed. (Munich: C. H. Beck, 2024), mn. 6.

¹⁷ See Maik Bäumerich, ‘Verschlüsselte Smartphones als Herausforderung für die Strafverfolgung: Neue Technologien, alte Befugnisse’ (2017) *Neue Juristische Wochenschrift* 2718–2722 at 2720.

¹⁸ See, for instance, Mathias Grzesiek and Daniel Zühlke, ‘Die Entschlüsselung von Smartphones gegen den Willen des Beschuldigten zum Zwecke der Durchführung des Strafverfahrens’ (2021) *Strafverteidiger-Spezial* 117; Andreas Grözing, ‘Anmerkung’ (2021) *Strafverteidiger-Spezial* 105.

¹⁹ BGBl. 2021 I, 2099.

premises and ‘if there is a concern that the data sought would otherwise be lost’ (§ 110 [3] 2 f. StPO). Yet, it is still an unresolved question of law whether this provision allows authorities to access storage media abroad without consent by the affected person (then: Article 32 [b] Convention on Cybercrime). While some argue that it suffices that such data is accessible from Germany,²⁰ and authorities regularly turn a blind eye to the question of where the data is located, others highlight that the German constitution requires German authorities to respect foreign sovereignty rights, which precludes a single-handed cross-border transfer of data.²¹ In any case, this provision is applicable only during the search of a premise – including the subsequent sifting through the data (§ 110 [3] 1 StPO, see Section 11.1.1.1) – and therefore subject to the same openness and transparency requirements.

In contrast, a provision enacted in 2017²² allows for ‘covert remote search[es] of information technology systems’ (§ 100b StPO): By using technical means, namely by infiltrating an information technology (IT) system, circumventing IT security measures and taking over control of such a system, an IT system of the accused (and of accomplices whose systems are used by the accused, § 100b [3] StPO) may be searched by the authorities and any data of interest may be extracted from it. This measure encroaches on a constitutional guarantee of preserving the confidentiality and integrity of information systems shaped in 2008 by the German Federal Constitutional Court in the context of preventive terrorism surveillance.²³ Owing to the highly intrusive nature of this measure, a number of safeguards are included. For instance, it is available only in investigations relating to those particularly serious crimes listed in § 100b [2] StPO; it requires judicial authorisation by a specific panel of three judges (§ 100e [2] StPO); those affected must be notified subsequently of the measure and given an opportunity for *ex post* judicial review (§ 101 StPO); and any data obtained is subject to a restrictive purpose-limitation regime (§ 100e [6] StPO). Moreover, technical means have to be employed to avoid obtaining any data relating to the ‘core area of the private conduct of life’ (§ 100d [3] 1 StPO) – such as data relating to innermost feelings, sexuality or religion – and any such data collected nonetheless is to be deleted immediately (§ 100d [3] 2 StPO). For the same reasons mentioned beforehand, such a measure is available only for information systems within the German territory – or where authorities presume that they are there.

11.1.1.3 Collecting Digital Evidence Concerning Telecommunication and Telemedia Usage

On constitutional grounds, a wiretap and other secret/clandestine investigation measures encroaching on the freedom of telecommunication (Article 10 Basic Law) require a specific legal basis, defining the scope, the material and procedural requirements as well as the safeguards for these measures.²⁴ The major such legal basis, § 100a StPO, was introduced in 1968 and in conjunction with a reduction of Allied Powers in Germany, to allow for wiretaps in criminal investigations.²⁵ To keep up with technical developments, but especially to expand the

²⁰ See Magda Wicker, ‘Durchsuchung in der Cloud. Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden’ (2013) *MultiMedia und Recht (MMR)* 765–769 at 768–769.

²¹ See Christian Rühls, *Durchsicht informationstechnischer Systeme* (Tübingen: Mohr Siebeck, 2022), 368–372 with further references.

²² BGBl. 2017 I, 3202.

²³ German Federal Constitutional Court, Judgment of 27 February 2008, 1 BvR 370, 595/07. On this judgment, see Christian Bumke and Andreas Voßkuhle, *German Constitutional Law: Introduction, Cases, and Principles* (Oxford: Oxford University Press, 2019), mn. 358–363.

²⁴ See generally German Federal Constitutional Court, Order of 3 March 2004, 1 BvF 3/02.

²⁵ See Dominik Brodowski, *Verdeckte technische Überwachungsmaßnahmen im Polizei- und Strafverfahrensrecht* (Tübingen: Mohr Siebeck, 2016), 158–161 with further references.

possibilities to collect digital evidence concerning telecommunication and ‘telemedia’ usage, the provisions in §§ 100a ff. StPO have been amended numerous times²⁶ and have, by now, created a complex haze of provisions in dire need of reform.²⁷ Another imminent change adds further complexity: on 15 January 2024, the German government tabled a bill in parliament²⁸ to implement the EU Digital Services Act.²⁹ One notable change it suggests relates to the terminology, as it seeks to rename ‘telemedia’ to ‘digital services’ in the text and title of various legal provisions, such as in §§ 100a ff. StPO.

The original provision on wiretaps in § 100a StPO has evolved into a provision justifying the surveillance of the *content* of all types of *telecommunication*, including internet usage,³⁰ stemming from and/or directed to a specific ‘connection’ or ‘end device’ (compare with §§ 100a [1], 100e [3] No. 5 StPO). As more and more communication transferred ‘over the wire’ is encrypted, § 100a StPO was expanded in 2017³¹ to permit the extraction of telecommunication ‘at the source’, that is, by infiltrating the end device and/or an application running on that system, as long as such a measure can be limited technically and organisationally to this purpose, and excessive data collections are thereby made impossible (§ 100a [1] 1 [5] StPO). If this technical measure can only be implemented with delay, § 100a [1] 2 StPO allows the extraction of such data which was transferred using telecommunication since the wiretap was ordered. Yet, this extension blurs the line to a ‘covert remote search of information technology systems’ (§ 100b StPO) and, similarly to § 95a [1] StPO, raises doubts from the perspective of constitutional guarantees.³²

A distinct legal provision addresses access to *telecommunication traffic data* (§ 100g StPO). It differentiates between traffic data which was stored by telecommunication providers for their own (e.g. technical) purposes as well as a ‘live’ capture of traffic data on the one hand (§ 100g [1] StPO) and traffic data stored in fulfilment of data retention obligations (§ 100g [2] StPO, see Section 11.1.2) on the other hand. If the query within the traffic data is based not on a specific customer or telephone number but on geographic location (a specific radio cell, and information about which devices were or are connected to it), the measure is subject to a stricter proportionality requirement; concretely, the extent of the data collection must be appropriate in relation to the importance of the criminal investigation (§ 100g [3] No. 2 StPO).

Since 2021, another distinction is clearly embedded into the German Code of Criminal Procedure: § 100g StPO relates only to *telecommunication traffic data*. Not covered by this provision are so-called telemedia services, which are ‘electronic information and communication services’ built ‘on top’ of telecommunication networks but which are neither

²⁶ For an overview, see Brodowski, ‘Überwachungsmaßnahmen’, 157–173.

²⁷ See Ulrich Sieber, *Straftaten und Strafverfolgung im Internet* (Munich: C. H. Beck, 2012), C103–C128; Nicolas von zur Mühlen, *Zugriffe auf elektronische Kommunikation. Eine verfassungsrechtliche und strafprozessrechtliche Analyse* (Berlin: Duncker & Humblot, 2019), 411–454.

²⁸ Deutscher Bundestag, Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze, BT-Drucksache 20/10031, dserver.bundestag.de/btd/20/100/2010031.pdf.

²⁹ Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services and amending Directive 2000/31/EC of 19 October 2022 (Digital Services Act) [2022] OJ L 277/1.

³⁰ German Federal Constitutional Court, Order of 6 July 2016, 2 BvR 1454/13.

³¹ BGBl. 2017 I, 3202.

³² See, for example, Mario Martini and Sarah Fröhlingsdorf, ‘Catch Me If You Can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik’ (2020) *Neue Zeitschrift für Verwaltungsrecht* 1803–1804.

telecommunication services nor radio/mass-media services (compare with § 1 [1] 1 *Telemediengesetz* – TMG). Based on a new provision,³³ § 100k StPO, usage data (*which user used what service at what time from what location*) pertaining to such ‘telemedia services’ may be collected by the authorities. According to jurisprudence, navigation services provided by modern cars are such a telemedia service; therefore, the location of the car – or, more precisely, of the subscriber identity module (SIM) card built into the car – may be collected from telemedia service providers on the basis of § 100k StPO.³⁴

The telecommunication-related measures mentioned previously relate to specific connections or end devices, but do not make a direct link to the user of these devices. To make such a connection, § 100j [1] 1 No. 1, 2 StPO provides a legal basis to obtain the ‘subscriber data’ relating to who contracted, for example, a SIM card or a digital subscriber line (DSL), including passwords, personal identification numbers (PINs) and access codes pertaining to the contracted service. Queries may also be made on the basis of a dynamically allocated internet protocol (IP) address and a specific time (§ 100j [2] StPO); to answer this query, the service provider may make use of traffic or usage data, including traffic data stored in fulfilment of data retention obligations.³⁵ In 2021, this provision was extended³⁶ to ‘subscriber data’ for telemedia services (§ 100j [1] 1 No. 2, 3 StPO), such as to collect credit card data with which a service was paid for, but also to obtain access codes to the telemedia service insofar as such codes may be used for further measures, such as surveillance of telecommunication.

Except for access to subscriber data, the aforementioned measures are all subject to substantial material and procedural limitations. Materially, these measures are available only in investigations of specific crimes (list offences, §§ 100a [2], 100g [2] 2, 100k [2] StPO), of crimes of at least substantial significance (§§ 100g [1] 1 No. 1, 100k [1] 1 StPO) and/or of crimes committed ‘by means of telecommunication’ (§ 100g [1] 1 No. 2 StPO) and they are subject to the principle of proportionality of the measure in light of their severity and potential alternative approaches to the criminal investigation. Procedurally, all these measures generally require *ex ante* judicial authorisation (§ 100e [1] 1 StPO, also in conjunction with § 101a [1], [1a] StPO), although three-day emergency authorisations (§ 100e [1] 2, 3 StPO, also in conjunction with § 101a [1], [1a] StPO) as well as limited requests to telemedia usage data (§ 100k [3] StPO) may be issued by public prosecutors. *Ex post*, the affected persons are to be notified, who then may request judicial review (§§ 101, 101a [6] StPO). The data acquisition is to be limited to protect, inter alia, the aforementioned ‘core area of private conduct of life’, but also constitutionally protected privileges such as the client–attorney privilege. To further curtail the effects of these measures, the data obtained is subject to a specific purpose-limitation regime: it may be used only in furtherance of other criminal investigations in case the (material) requirements to order the measure anew are hypothetically met in that other investigation (§ 479 [2] 1 StPO in conjunction with § 161 [3] StPO).

Notably, though, the provisions in the German Code of Criminal Procedure relate only to the collection of data by law enforcement authorities (LEAs). According to the jurisprudence by the German Federal Constitutional Court referring to a ‘requirement of two doors’, any transfer of data originally acquired by service providers for other means – such as to provide

³³ BGBl. 2021 I, 448, 1380.

³⁴ Oberlandesgericht Frankfurt (Higher Regional Court of Appeals Frankfurt), Order of 20 July 2021 – 3 Ws 369/21; see also the critical assessment by Felix Ruppert, ‘Anmerkung’ (2022) *Strafverteidiger-Spezial* 70.

³⁵ German Federal Constitutional Court, Order of 24 January 2012, 1 BvR 1299/05.

³⁶ BGBl. 2021 I, 448, 1380.

telecommunication services – additionally requires a legal basis in telecommunication or telemedia law.³⁷ As these provisions (such as the TTDSG, the TMG and the TKG; see, in more detail, Sections 11.3.3.2–11.3.3.4) are enacted on the federal level as well, the legislature usually keeps these provisions in coordination.

11.1.2 Data Retention Obligations: Legal Framework, Practice and Challenges

Taking effect on 1 January 2008,³⁸ Germany implemented the Data Retention Directive 2006/24/EG by introducing an obligation for service providers (access providers, email providers and classic telecommunication providers) to retain traffic data for six months (§ 113a *Telekommunikationsgesetz* [TKG] as of 1 January 2008), a generic rule that this retained data may be used, inter alia, to prosecute crimes (§ 113b TKG as of 1 January 2008) and a specific legal basis for accessing this data in criminal investigations (§ 100g StPO as of 1 January 2008). It was meant to be available for the investigation of all crimes of at least substantial significance or committed ‘by means of telecommunication’, yet the access to retained data generally required judicial authorisation.

Owing to much criticism against data retention which had been voiced in the German legal and political discourse, around 34,000 citizens lodged a constitutional complaint against these provisions, in the first-ever mass complaint lodged with the German Federal Constitutional Court. On 2 March 2010, it pointed out that the European Court of Justice (ECJ) had not (yet) nullified the Directive,³⁹ and assessed that a six-month general data retention of telecommunication traffic data is not unconstitutional as such, but its implementation must be proportionate. Therefore, to collect such retained data in a criminal investigation, there must be a concrete suspicion of a severe crime; as the retained data contains sensitive information, a sufficient level of data security and data protection must be prescribed by law. As the German implementation in §§ 113a, 113b TKG and § 100g StPO did not meet these safeguards, the court declared these provisions to be unconstitutional and void.⁴⁰ Without a (constitutional) legal basis, such telecommunication traffic data could no longer be retained by German service providers – except for technically necessary retaining of traffic data for a few days or at most a fortnight. Such data is, up to today, oftentimes requested by LEAs on the less strict legal basis of § 100g [1] StPO.

That found Germany in the situation where it violated its implementation obligation, and the European Commission launched infringement proceedings which only came to a halt⁴¹ once the ECJ had declared the Directive 2006/24/EG invalid.⁴² Notwithstanding that, in 2015 Germany enacted a renewed data retention obligation that is more limited in scope and tries to take the requirements set out by the German Federal Constitutional Court into account.⁴³ In particular, these provisions to retain traffic data (now: §§ 175 ff. TKG 2021) were limited to providers of voice communication services and internet access providers, the retention period was limited to ten weeks (four weeks for location data) and access for criminal investigations was limited to those particularly serious crimes listed in § 100g [2] 2 StPO.

Referring to the evolving ECJ jurisprudence on national data retention laws, the conformity of these new provisions with Union law was soon cast into doubt. A few days before the data retention requirements took effect, and based on an interim relief granted by an administrative

³⁷ First coined in German Federal Constitutional Court, 1 BvR 1299/05.

³⁸ BGBl. 2007 I, 3198.

³⁹ Case C-301/06, *Ireland v. Parliament and Council* [2009] ECR I-00593, ECLI:EU:C:2009:68.

⁴⁰ German Federal Constitutional Court, Judgment of 2 March 2010, 1 BvR 256, 263 and 586/08.

⁴¹ Case C-329/12, *Commission v. Germany* [2014] ECLI:EU:C:2014:2034.

⁴² Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:238.

⁴³ BGBl. 2015 I, 2218.

court,⁴⁴ the responsible government agency *Bundesnetzagentur* decided that it will not enforce these requirements until a final court decision.⁴⁵ Complaints by service providers lodged in administrative courts led to a preliminary ruling request judged by the ECJ on 20 September 2022,⁴⁶ with national courts subsequently confirming that the German framework on data retention is incompatible with Union law and therefore must not be enforced.⁴⁷

In the political arena, the current coalition agreement includes a statement that the parties represented in the German government intend to modify the rules on data retention, based on the upcoming ruling by the ECJ, to allow for an ad hoc retaining of data based on a judicial order. Moreover, the agreement proposes to introduce a ‘login trap’ as an alternative to data retention,⁴⁸ which would work as follows: If authorities want to track down a user in a social network, they order the service provider to set the specific user a ‘trap’. At the user’s next login, this ‘trap’ triggers and exposes the user’s current IP address to the authorities. Using this current IP address, the authorities then issue a request for subscriber data to the relevant access provider. If this request is issued soon enough (or automatically), the access provider will be able to resolve the IP address to the user’s subscriber data even without any data retention obligation. While this approach may indeed prove useful for investigating ordinary crimes on social media – such as hate speech – its utility is far more tailored compared to a generic data retention requirement.⁴⁹

11.2 TERMINOLOGY AND CATEGORISATIONS

11.2.1 *Data*

11.2.1.1 Terminology

German criminal procedure does not define ‘data’ or ‘digital evidence’ (see Section 11.1). Instead, some provisions make use of more general terms, such as § 94 StPO, where the term ‘objects’ refers to tangible objects (including data storage devices) as well as to any ‘data’ as such (see Section 11.1.1.1). In a similar vein, the provision on ‘covert remote search[es] of information technology systems’ (§ 100b StPO) generally allows the collection of any ‘data’ present on such systems. Other provisions refer to more specific categories of data, such as ‘telecommunications’ to be intercepted (§ 100a StPO), ‘subscriber data’ (§ 100 j StPO) and ‘traffic data’ (§ 100g StPO) as defined in telecommunications and telemedia law, and ‘personal data’ as defined in data protection law. This approach allows for coherence within national law and is – insofar as very generic terms such as ‘objects’ are used – technology-neutral. Yet, some ambiguities remain, in particular where the terms used in the legislation seem to refer only to tangible objects (such as a requirement to ‘surrender’ an object, § 95 [1] StPO), or where it is unclear whether surfing the internet is correctly labelled as ‘telecommunications’ within the meaning of telecommunication surveillance (see Section 11.1.1.3).

⁴⁴ Oberverwaltungsgericht Nordrhein-Westfalen (Higher Administrative Court Northrhine-Westphalia), Order of 22 June 2017, 13 B 238/17.

⁴⁵ See Verkehrsdatenspeicherung, Bundesnetzagentur, www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/OeffentlicheSicherheit/Ueberwachung_Auskunftsert/VDS_113aTKG/node.html.

⁴⁶ Joined Cases C-793/19 and C-794/19, *SpaceNet and Telekom Deutschland* [2022] ECLI:EU:C:2022:702.

⁴⁷ Bundesverwaltungsgericht (German Federal Administrative Court), Judgment of 14 August 2023, 6 C 6/22, ECLI:DE:BVwG:2023:140823U6C6.22.o.

⁴⁸ ‘Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit’ (Coalition Agreement 2021–2025), 109, www.bundesregierung.de/breg-de/service/gesetzesvorhaben/koalitionsvertrag-2021-1990800.

⁴⁹ For an extensive analysis, see Dominik Brodowski, ‘Die “Login-Falle” zur Identifizierung von Beschuldigten im Internet – eine “grundrechtsschonende und freiheitsorientierte” Ermittlungsmaßnahme?’ (2022) *Strafverteidiger* 413.

11.2.1.2 Categorisation

The German Code of Criminal Procedure differentiates between (telecommunication) traffic data (including location data), (telemedia) usage data (including location data) and (telecommunication and telemedia) subscriber data. In the specific legal provisions on the collection of such data, the code refers to the specific definitions contained in telecommunications and telemedia law, namely:

- *telecommunications traffic data* (§ 100g [1] 1 StPO) as defined in §§ 9 and 12 in the Act on the Protection of Personal Data and Privacy in Telecommunication and Telemedia (*Telekommunikation-Telemedien-Datenschutz-Gesetz* – TTDSG) and § 2a [1] BDBOSG (an act relating to telecommunications by LEAs and rescue services), with a further differentiation according to whether retained data is collected. In particular, dynamic IP addresses assigned by access providers are considered to be *traffic data*, although using that data indirectly, when querying for subscriber data based on an IP address and a specific time, is merely subject to the provisions on collecting subscriber data (§ 100j StPO, see Section 11.1.1.3);
- *telemedia usage data* (§ 100k StPO) as defined in § 2 [2] No. 3 TTDSG, with simplified access to usage data solely relating to identification of the user (§ 100k [3] StPO in conjunction with § 2 [2] No. 3 lit. a TTDSG); and
- *subscriber data* (§ 100j [1] 1 StPO) as defined in §§ 3 No. 6, 172 TKG and § 2 [2] No. 2 TTDSG, with a further differentiation for authentication data protecting end devices and storage devices, such as login information, passwords and PINs (§ 100j [1] 2 StPO).

In contrast, telecommunication *content* data is not defined in German criminal procedure. Instead, the provision of telecommunication (content) surveillance (§ 100a StPO) is interpreted to cover all telecommunication in a technical sense (§ 3 No. 59 TKG). In particular, this broad approach includes chat messages and emails (read and unread), communication in the context of online games as well as machine-to-machine data, as it is generally impossible to distinguish between different types of content already when collecting the data.⁵⁰ In contrast, data which has not yet been transferred between computers and networks, such as draft emails or decryption keys, is not telecommunication content data. Instead, such data may only be seized openly (§ 94 StPO) or collected using a ‘covert remote search of information technology systems’ (§ 100b StPO).

The aforementioned differentiations build upon distinctions made in telecommunication and telemedia law. These distinctions are heavily predetermined by EU law such as the EU Electronic Communications Code, Directive (EU) 2018/1972.

11.2.2 Service Providers

The German Code of Criminal Procedure does not define ‘service providers’ as such. Instead, provisions setting out cooperation requirements refer to (natural and legal) persons providing or collaborating in the provision of specific services, partly under the additional requirement that such provision or collaboration must be done on a commercial basis:

- For telecommunication content surveillance (§ 100a [4] 1 StPO) and collection of traffic data (§ 100a [4] 1 StPO in conjunction with § 101a [1] StPO), reference is made to persons who provide or collaborate in the provision of telecommunication services.

⁵⁰ Compare with von zur Mühlen, ‘Elektronische Kommunikation’, 118–141.

- For collecting subscriber data (§ 100j [5] 1 StPO), reference is made to persons who provide or collaborate in the provision of telecommunication or telemedia services.
- For collecting telemedia usage data, reference is made to persons who, on a commercial basis, make telemedia available for use or who mediate such services (§ 100k [1] 1, 101a [1a], 100a [4] 1 StPO).

While the term ‘social media providers’ is not used in the German Code of Criminal Procedure, it is central to a specific Act on Law Enforcement in Social Networks (*Netzwerkdurchsetzungsgesetz* – NetzDG). This Act applies to ‘digital service providers’ that provide, with the intention of profit, platforms on the internet intended to enable users to share any content with other users or make it available to the public (§ 1 [1] 1 NetzDG), unless these platforms provide journalistic content or are focused on bilateral exchanges or on the dissemination of specific content (§ 1 [1] 2 and 3 NetzDG).

By focusing on the *service* being provided – and implicitly on the underlying regulation and definition of telecommunication services in accordance with the EU Electronic Communications Code in § 3 No. 1, 61 TKG – this approach is both broad and coherent with supranational as well as telecommunication and telemedia law. However, not all delineations between telecommunication and telemedia (as well as social media) services are clear-cut. For instance, the social media platforms Facebook and X may be used for private direct messages between two users – where it constitutes an (interpersonal) telecommunication service – and for messages directed to the masses – where it then constitutes a telemedia service. It is unclear how to proceed if, for instance, usage/traffic data is to be obtained from such a service provider but it is unknown whether the relevant user used the service in one or the other manner.⁵¹

11.3 DOMESTIC COOPERATION BETWEEN LEAs AND SERVICE PROVIDERS

11.3.1 *Introduction*

Hand in hand with the increased digitisation of society, German LEAs put ever more emphasis on cooperation with service providers and on creating and enforcing laws requiring their assistance in criminal investigations. Obviously, such cooperation is of particular importance for certain types of crime, such as online hate crimes. However, as digital evidence becomes ever more widespread in *all* types of crime, cooperation duties are usually not limited to specific cybercrime or IT-related offences.

Traditionally, the focus of any such cooperation requirements were ‘wholly domestic’ situations where the service was provided in Germany, by a service provider seated in Germany, and the data of interest was present within Germany. In such situations, requiring the service provider to hand the data over to LEAs is fully in line with the traditional notion of full state authority within its territory. Although no clear references are available in the case law or in secondary sources, cooperation by service providers was also requested in ‘partially domestic’ situations where the service provider was seated within Germany and offered the service domestically, but where the service provider might have needed to transfer the requested data to Germany first.

However, in December 2021 a groundbreaking reform of the telecommunication and telemedia service regulation entered into force,⁵² with effects on criminal procedure that had not

⁵¹ See, in more detail, Brodowski, ‘Login-Falle’, 416.

⁵² BGBl, 2021 I, 1858 and 1982.

been considered during the parliamentary proceedings.⁵³ This reform leads to a ‘domestication’ of foreign service providers, by stating that the laws regulating the provision of telecommunication and telemedia services in Germany apply to such services offered in Germany (§ 1 [2] TKG, § 1 [3] TTDSG), regardless of whether the service provider and their technical infrastructure is located in Germany. Taken literally, this *lex loci solutionis* approach also applies to requirements that service providers must fulfil (lawful) requests by LEAs for content, traffic, usage and/or subscriber data (§§ 170–183 TKG, §§ 22–24 TTDSG), without any involvement of foreign authorities.⁵⁴ However, it has not yet been evaluated by courts whether such extraterritorial effects are actually lawful under German constitutional law – which pays much attention to be in accordance with international law and therefore not to infringe upon the sovereignty of other countries (see Sections 11.4.1 and 11.4.2.2) – and Union law. These doubts are further fuelled by court decisions in relation to a reporting obligation enacted as § 3a NetzDG: Two service providers seated in other EU member states filed a claim against the authority tasked with the supervision and enforcement of this obligation – the Federal Office of Justice (*Bundesamt für Justiz*) – with the administrative court in Cologne; it has jurisdiction as the authority is seated within its district. This court held that the German reporting obligation may violate the ‘home state regulation’ principle set out in the Electronic Commerce Directive 2000/31/EG and, in particular, its Article 3[2] stating that ‘Member States may not, for reasons falling within the coordinated field, restrict the freedom to provide information society services from another Member State’. Therefore, it granted intermediate relief, stating that the petitioning service providers are not bound by the reporting obligation vis-à-vis the enforcement authority.⁵⁵ However, § 3a NetzDG is suggested to be repealed by the aforementioned legislative proposal to implement the EU Digital Services Act (see Section 11.1.1.3).

11.3.2 Nature of the Cooperation

Law enforcement agencies may ask for and receive *informal voluntary* cooperation by service providers based on the generic legal basis for criminal investigations (§§ 161, 163 StPO), unless such cooperation is contrary to the law⁵⁶ or the cooperation, as it substantially encroaches into human and fundamental rights of third parties, requires a more specific legal basis.⁵⁷ From the perspective of service providers, the major boundaries to voluntary cooperation with LEAs are the protection of the secrecy of telecommunications, as stipulated in § 3 TTDSG and also enforced by means of criminal law (§ 206 German Penal Code [*Strafgesetzbuch – StGB*]), and the protection of personal data in accordance with the General Data Protection Regulation (GDPR) and the accompanying Law Enforcement Directive (EU) 2016/680 including its implementation in Germany. Therefore, voluntary cooperation is the exception rather than the rule, and may be more prominent insofar as it relates to technical background information instead of personal data.

The typical mode of ‘cooperation’ between LEAs and service providers is *mandatory* and *enforceable*, meaning that service providers are compelled by a specific and clear provision in the law to fulfil a lawful request made by the authorities. In case they wrongfully violate this

⁵³ Compare with Brodowski, ‘Login-Falle’, 417–418.

⁵⁴ *Ibid.*, 416.

⁵⁵ Verwaltungsgericht Köln (Administrative Court Cologne), Order of 1 March 2022 – 6 L 1354/21; Administrative Court Cologne, Order of 1 March 2022 – 6 L 1277/21.

⁵⁶ Sieber and Brodowski, ‘19.3 Strafprozessrecht’, mn. 101.

⁵⁷ *Ibid.*, mn. 100.

requirement, authorities can compel the service providers to perform, utilising the administrative measures and means of compulsion set out in § 70 StPO (in conjunction with §§ 95 [2], 100a [4] 3, 100j [5] 2 StPO), that is (for natural persons) detention of up to six months (§ 70 [2] StPO) and (for natural and legal persons) a fine of up to 1,000 EUR (§ 70 [1] 2 StPO, Article 6 [1] EGStGB) per case.⁵⁸ Besides these measures, which are directed at the (delayed) performance of the request, service providers and/or the natural persons acting on their behalf may be sanctioned for their (past) violation (§§ 9 OWiG, 14 StGB). Depending on the circumstances, they may have to pay an administrative fine for violating specific administrative offences targeting cooperation requirements (see, in particular, § 228 [2] No. 39, 42–61 TKG) or, if done with the direct intent to impede the investigation, may face imprisonment or a fine under criminal law for obstruction of prosecution (§ 258 StGB). It should be noted, however, that the execution of these compelling measures or sanctions may be difficult or even impossible for foreign but ‘domesticated’ service providers (see Section 11.3.1), even if they have an office or representation in Germany. The provider might have authorised the German office only to *receive* requests by LEAs, but might not have granted it the means to *access* the requested data. Under such conditions, the representation in Germany cannot be compelled to provide data or sanctioned for the non-provision of data: *impossibilia nulla est obligatio*.

A newer but evolving mode of *mandatory* ‘cooperation’ is reporting duties where service providers, once they become aware of a specific incident, have to report the incident and data relating to it proactively to the authorities. Besides a generic reporting obligation relating to specific, planned crimes which may yet be averted (§ 138 StGB, see Section 11.3.3) – and reporting obligations under Anti-Money-Laundering provisions and under the GDPR which are outside the scope of the present chapter – § 3a NetzDG contains a specific and enforceable reporting obligation for large-scale social network providers (see Section 11.3.4).

11.3.3 Overview of Existing Cooperation Duties

German law does not know of an all-encompassing cooperation requirement in relation to criminal investigations and prosecutions. Instead, any such requirement needs a specific and precise legal basis, as any compelling to action encroaches on the constitutionally protected general freedom of action (Article 2 [1] Basic Law) and/or occupational freedom (Article 12 Basic Law).

However, there is a legal basis in German criminal procedure that *anyone* can be compelled to provide witness statements to the courts, to public prosecutors and, upon specific authorisation, also to the police (§ 163 [3] StPO). To avoid being called as a witness to the police and/or the prosecutor, a witness can submit a written statement. Notably, witnesses generally have no duty to prepare themselves for their statement; instead, they are required only to appear, to potentially swear an oath and to give their statement of their own observations (including their own thoughts and feelings). Yet automated technical activities – such as data processing operations at a service provider – are typically not observed by humans. Therefore, these can only exceptionally become relevant in a witness statement if the witness has observed the input or the output of data processing themselves.

⁵⁸ See, for instance, German Federal Constitutional Court, Order of 20 December 2018, 2 BvR 2377/16; Landgericht München (Regional Court Munich), Order of 4 December 2019, 9 Qs 15/19.

Additionally, there is a generic reporting obligation which follows from a provision in criminal law, § 138 StGB. It criminalises the failure to report a planned serious offence specifically listed in that provision (such as high treason, murder or robbery) at a time when this offence could still have been averted. This provision prevails over the privacy of telecommunication.⁵⁹ That means that if, for example, a worker with a telecommunication service provider debugs an email service and then, by chance, becomes aware of planned murder, they have to report it to the authorities or face criminal prosecution and imprisonment themselves.

11.3.3.1 Cooperation Duties of Possessors of Objects

Another quite generic cooperation duty exists in relation to possessors of objects which are of interest to a criminal investigation. Based on § 95 [1] StPO, LEAs may order the possessor (except suspects or accused persons) to ‘surrender’ this object to the authorities. As it is generally an ‘open’ investigation measure, suspects must be informed of such a measure speedily unless a specific ‘gag order’ based on § 95a [6] StPO is issued (see Section 11.1.1.1).

This so-called production order is available in all criminal investigations and limited only by the principle of proportionality. Even though the law is not perfectly clear on this issue, and legal practice does not consider a judicial warrant (§ 98 [1] StPO) to be necessary, it is oftentimes issued upon request by service providers. Although the wording is slightly ambiguous, this measure is commonly understood to relate also to any data⁶⁰ in the possession of a non-suspect, including data relating to past or ongoing telecommunications, unless access to such data is governed by more specific provisions.⁶¹ Importantly, § 95 [1] StPO requires only the ‘production’ of specific objects already in existence at the time of the request: it is a legal basis neither for the creation of new data nor for the analysis or conversion of data.⁶²

Owing to this limitation, § 95 [1] StPO is, as such, no legal basis on which to order the decryption of data. If stored somewhere, however, the password or key file necessary to decrypt data may be obtained by means of § 95 [1] StPO; if known to a non-suspect, that person can be called as a witness to testify on their observations of the password.⁶³ *A maiore ad minus*, many service providers agree to (voluntarily) decrypt data themselves or to preprocess it themselves, to avoid being called as a witness and/or to avert the seizure of larger amounts of data.

As § 95 [1] StPO builds upon the German law on search and seizure, this measure is available only insofar as German authorities could lawfully seize objects – including data – themselves. Therefore, authorities cannot order the disclosure of data which is located in another country, as any seizure of such objects would violate foreign sovereignty and also the constitutional guarantee to adhere to the principles of international law (Article 25 Basic Law). This limitation of Germany’s jurisdiction to enforce cannot be circumvented by ordering private parties to act on Germany’s behalf.⁶⁴

⁵⁹ Just see Detlev Sternberg-Lieben, ‘§ 138 StGB – Nichtanzeige geplanter Straftaten’, in Albin Eser et al. (comm.), *Schönke/Schröder. Strafgesetzbuch*, 30th ed. (Munich: C. H. Beck, 2019), mn. 25.

⁶⁰ German Federal Constitutional Court 2 BvR 1027/02; German Federal Constitutional Court, 2 BvR 372/01.

⁶¹ German Federal Constitutional Court, 2 BvR 902/16.

⁶² Sieber and Brodowski, ‘19.3 Strafprozessrecht’, mn. 103; von zur Mühlen, ‘Elektronische Kommunikation’, 355, 394.

⁶³ Sieber and Brodowski, ‘19.3 Strafprozessrecht’, mn. 110–112; von zur Mühlen, ‘Elektronische Kommunikation’, 353–354.

⁶⁴ Sieber and Brodowski, ‘19.3 Strafprozessrecht’, mn. 104; Ulrich Sieber and Carl-Wendelin Neubert, ‘Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty’ (2017) 20 *Max Planck Yearbook of United Nations Law* 239–321 at 275–277.

11.3.3.2 Cooperation Duties of Telecommunication Service Providers

For the surveillance of telecommunications as well as the collection of telecommunication traffic and subscriber data, there is an extensive legal framework for the cooperation duties of telecommunication service providers: Within the German Code of Criminal Procedure, § 100a [4] 1 StPO sets out that, if an interception of telecommunication has been ordered (see Section 11.1.1.3), anyone who provides or collaborates in the provision of telecommunication services has to enable the execution of such an order and to provide any necessary information without undue delay.⁶⁵ The same provision applies, *mutatis mutandis*, for the collection of telecommunication traffic data (§ 101a [1] 1 StPO), with the additional tweak that the service provider has to inform the authorities which information stems from data stored based on the requirements of data retention. A slight difference exists concerning the collection of telecommunication subscriber data: there, the cooperation duty extends only to those who provide or collaborate in the provision of telecommunication services on a commercial basis. This provision explicitly mentions that they have to transmit the requested data without undue delay (§ 100j [5] 1 StPO).

As referenced in § 100a [4] 2 StPO, the TKG and an ordinance adopted on its basis – the Telecommunication Interception Ordinance (TKÜV) – set out in further detail whether and what preparations (domestic or domesticated, see Section 11.3.1) telecommunication service providers have to make so that orders for the interception of telecommunications can be executed speedily; additionally, a federal agency, the *Bundesnetzagentur*, is empowered to set out technical directives (TR TKÜV) with further details. For instance, § 170 [1] 1 No. 1 TKG requires those operating a telecommunications system that is used for publicly accessible telecommunication services to maintain, at their own expense, the technical facilities necessary to intercept telecommunications and to take organisational precautions for their immediate implementation upon request. According to § 170 [11], TKG providers of public mobile phone networks must ensure that, in case of roaming, ‘any encryption applied by the foreign operator on the network side’ is removed, insofar as there are international technical standards available to that end.

In 2018, the German Federal Constitutional Court held that these cooperation duties, while encroaching on the service providers’ right to occupational freedom (Article 12 Basic Law), are constitutional, even if they require ‘data protection-friendly’ service providers to modify their technical infrastructure. One German provider had stated that it employs a network-address-translation (NAT) technology so that it does not and cannot log the IP address relating to a user accessing a specific email account, and therefore refused to implement a court order on the interception of that user’s telecommunication. However, the German Federal Constitutional Court pointed out that the IP address is actually processed by the provider at the NAT stage, and thus such actions can be required, even if the service provider may need to restructure and reprogram its infrastructure. As the service provider had failed to do so, the issuance of a compulsory fine of 500 EUR was held to be constitutional as well.⁶⁶

11.3.3.3 Cooperation Duties of Telemedia Service Providers

Concerning telemedia service providers, the law is structured similarly: § 101a [1a] StPO in conjunction with § 100a [4] StPO stipulates that anyone who provides or collaborates in the provision of telemedia services has to enable the execution of an order requesting usage data

⁶⁵ See extensively von zur Mühlen, ‘Elektronische Kommunikation’, 270–313.

⁶⁶ German Federal Constitutional Court, 2 BvR 2377/16.

(§ 100k StPO) and to provide any necessary information without undue delay. The personal scope is further limited, however, by § 100k [1] 1 StPO, which states that such information may be collected (only) from those who, on a commercial basis, make telemedia available for use or who mediate such services. The cooperation duty with regard to the collection of telemedia subscriber data (including password data) extends to those who provide or collaborate in the provision of telemedia services on a commercial basis, and explicitly sets out that they have to transmit the requested data without undue delay (§ 100j [5] 1 StPO).

These provisions of criminal procedure are further complemented by §§ 22–24 TTDSG, which stipulate that those who provide or collaborate in the provision of telemedia services on a commercial basis have to cooperate with LEAs requesting data according to §§ 100j, 100k StPO. In particular, they have to transfer the requested data without undue delay (§§ 22 [5] 1, 23 [3] 1, 24 [4] 1 TTDSG) and to keep silent about such requests (§§ 22 [5] 3, 23 [3] 3, 24 [4] 3 TTDSG). It is further clarified that any encryption of the requested data remains unaffected (§§ 22 [5] 2, 23 [3] 2, 24 [4] 2 TTDSG), meaning that service providers are not and must not be compelled to weaken or circumvent any encryption employed by the users of their services. Service providers furthermore have to make preparations, at their own expense, so that they process requests, and they furthermore have to assert that a specialist verifies, before releasing the requested information, that the LEAs issued a formally valid order (§§ 22 [6], 23 [4], 24 [5] TTDSG). Nevertheless, failures to make such preparations are not subject to sanctions.

11.3.3.4 Cooperation Duties of Social Media Providers

For *all* social media providers (see Section 11.2.2), regardless of where they are seated, § 5 [2] NetzDG requires that they specify a person responsible to receive requests by LEAs. This person has to respond within forty-eight hours (§ 5 [2] 2 NetzDG), and if the response to the request is not sufficient to fulfil the request, the response has to be reasoned (§ 5 [2] 3 NetzDG). Only the failure to specify a person and the failure to respond are sanctionable as administrative offences – even if committed outside of Germany (§ 5 [3] NetzDG) – and each bears a sanction of up to 500,000 EUR (§ 4 [1] No. 8 and 9, [2] NetzDG).

Since March 2022, and under the threat of an administrative sanction of up to 5 million EUR (§ 4 [1] No. 7, [2] NetzDG), § 3a NetzDG requires social media providers with more than two million registered users in Germany (§ 1 [2] NetzDG) to set up an effective procedure for reporting illegal content: If illegal content has been reported to the service provider – for example, a user reporting a message containing criminal hate speech – and the service provider deletes or removes access to that content based on obligations under § 3 NetzDG, it has to assess whether there are concrete indications that, by disseminating the content, at least one of the criminal offences listed in § 3 [2] No. 3 NetzDG has been violated (such as dissemination of propaganda material of unconstitutional organisations [§ 86 StGB], disturbing public peace by threatening to commit offences [§ 126 StGB], rewarding and approval of offences [§ 140 StGB] and dissemination, procurement and possession of child pornography [§ 184b StGB]). If so, it has to report the content and related metadata, including the IP address and the transmission control protocol (TCP)/user datagram protocol (UDP) port of the user's last access to the social network, electronically to the Federal Criminal Police Office (*Bundeskriminalamt*). Unless ordered to continue the silence, the service provider has to inform the user, once four weeks have elapsed, that their data has been transmitted. This reporting obligation is severely limited, however, by

the aforementioned court injunctions stating that its design was incompatible with the ‘home state regulation’ principle set out in the Electronic Commerce Directive 2000/31/EG.⁶⁷

The EU Digital Services Act enacted in 2022 removes Germany’s need – and ability – to regulate these cooperation duties of social media providers. Therefore, the aforementioned legislative proposal (see Section 11.1.1.3) seeks to repeal these provisions of the NetzDG.

11.3.4 *Legal Remedies and Protection of Fundamental Rights*

Insofar as cooperation requests have legal effects on service providers – which is not the case if LEAs merely ask for voluntary cooperation – they enjoy the constitutionally protected right to legal review (Article 19 [3] Basic Law). In particular, they can appeal to courts against orders by the police or public prosecutors to the courts (§ 98 [2] 2 StPO), appeal against court decisions (e.g. ordering the interception of telecommunications) to a higher court (§ 304 StPO) and lodge complaints to the German Federal Constitutional Court if they consider their basic rights to be violated. However, any such review is limited to the rights of the service providers. In particular, they have no standing to challenge the legality of a measure for lack of suspicion against the suspect, and oftentimes do not have sufficient information – and cannot have access to the case file – to properly evaluate this aspect. Instead, their standing to challenge is limited to the questions (a) whether the requirements for cooperation set out in law are met, (b) whether a specific action can be required from them under a specific statute – such as modifying their technical infrastructure to log IP addresses of their users⁶⁸ – and (c) whether the cooperation requirements are proportionate encroachments of their constitutionally protected general freedom of action (Article 2 [1] Basic Law) and/or occupational freedom (Article 12 Basic Law).

The rights – including the fundamental rights – of suspects, accused and affected third parties (such as those persons a suspect communicates with) are protected independently of the actions and omissions of the service provider instead. First of all, the legal bases of the aforementioned – in particular covert – measures contain material limitations to their scope, and procedural safeguards such as (regularly) a need for an *ex ante* judicial authorisation (see Section 11.1.1.3). Furthermore, suspects and other affected parties regularly are to be notified subsequently of covert measures as soon as that can be done without interfering with the ongoing investigation (§§ 95a [4], 100j [4], 101 [4] to [6], 101a [6] and [7] StPO) and given the opportunity to request an *ex post* judicial review of the measure (see, in particular, §§ 95a [5], 101 [7] 2–4, 101a [6] 2 StPO) and appeal such a decision to a higher court (§ 304 StPO).

11.4 CROSS-BORDER COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

11.4.1 *Introduction*

Owing to its peculiar history, Germany is very sensitive to adhering to the general principles of international public law – which, according to Article 25 Basic Law, are embedded into Germany’s law and precede laws enacted by parliament – and not to infringe upon the sovereignty of other countries. In line with this, the jurisdiction to enforce is generally interpreted to be restricted to Germany’s territory. Although the Act on International Mutual

⁶⁷ Administrative Court Cologne, 6 L 1354/21; Administrative Court Cologne, 6 L 1277/21.

⁶⁸ German Federal Constitutional Court, 2 BvR 2377/16.

Assistance in Criminal Matters (*Gesetz über die internationale Rechtshilfe in Strafsachen* – IRG) is silent on this matter, the administrative regulation on this matter (*Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten* – RiVAST) is explicit: German LEAs may get into direct contact with persons abroad only if it is not to be expected that the foreign country would object to this contact as an impermissible encroachment on its sovereign rights (No. 121 [1] 1 RiVAST). Accordingly, acknowledgements of receipts or notifications on the closing of a criminal investigation are considered to be unproblematic (No. 121 [1] 2 RiVAST). Yet – barring special provisions of international law – it is explicitly illegal to contact persons abroad and request some action or omission under the threat of any enforcement measures or other legal disadvantages (No. 121 [4] lit. a RiVAST).

Although a shift to a more service-oriented approach (see Section 11.3.1) and to the question of accessibility from Germany (see Section 11.1.1.2) can be noticed recently, and authorities sometimes turn a blind eye on this question, it is the physical location of the data at interest which determines whether a situation is domestic or whether it warrants cross-border cooperation (see Section 11.3.3.1). Yet, neither German criminal procedure nor German telecommunications or telemedia law currently contains data localisation requirements; instead, such questions may be governed by European provisions, in particular the GDPR.

11.4.2 Cooperation of National LEAs with Foreign Service Providers

11.4.2.1 Mediated Cooperation

Germany relies heavily on international, regional and supranational legal frameworks for mutual legal assistance (MLA). In particular, Germany is a party to, inter alia, the United Nations Convention against Transnational Organized Crime, the European Convention on Mutual Assistance in Criminal Matters and its first two additional protocols, the Convention on Cybercrime and its first additional protocol, and it is bound – by its membership to the EU – to implement the European Investigation Order (EIO). By and large, these instruments all are based on an interaction between LEAs in both countries involved, not on ‘direct action’ in a foreign state or direct cooperation with foreign private entities.

As the human and fundamental rights enshrined in Germany’s Basic Law are binding to Germany’s authorities also in cross-border situations,⁶⁹ it follows from constitutional law that a sufficient legal basis in German law is necessary for requesting MLA from other countries, including EU member states. In contrast to that, the normative framework on outgoing requests for MLA is rather weak. Still, and with a normative basis in § 77 [1] IRG, it is commonly accepted that the same material and procedural requirements must be met for an outgoing request as for conducting an investigation measure within Germany.⁷⁰ Therefore, to request, for example, telecommunication traffic data from a foreign service provider, an equivalent judicial order based on §§ 100g, 101a [1], 100e [2] StPO is required as in a comparable domestic situation. This domestic order may then provide the basis for an EIO or for a request for MLA sent to a foreign country. Moreover, this court order can be challenged in German courts – same as in a domestic situation – and serves to protect the fundamental rights of the affected parties.

⁶⁹ German Federal Constitutional Court, Judgment of 19 May 2020, 1 BvR 2835/17.

⁷⁰ Dominik Brodowski, ‘Vor §§ 68 ff. IRG’, in Heinrich Grützner and Paul-Günter Pötz (founders), *Internationaler Rechtshilfeverkehr in Strafsachen*, 136th supplement (Heidelberg: C. F. Müller, 2024), mn. 18–19 with further references.

11.4.2.2 Unmediated Cooperation

As stated in Section 11.4.1, unmediated cooperation with foreign service providers is necessarily voluntary – otherwise, it would contradict the constitutionally guaranteed protection of foreign sovereignty, and evidence obtained in violation thereof might not be available to prove a defendant's guilt.⁷¹ Nonetheless, in the regulation of telecommunication and telemedia service providers, the German legislature set out to enact a 'domestication' of foreign service providers, which – on its face – seems to allow unmediated and binding requests to foreign service providers offering their services on the German market. However, the conformity of this 'domestication' with constitutional and European law is still unclear (see Section 11.3.1).

Even if the cooperation with a foreign service provider is voluntary, the request by German authorities must still be lawful and, in particular, in line with the constitutionally required legal basis for collecting (personal) data. That means that also for a voluntary and unmediated cooperation between German LEAs and foreign service providers, the same material and procedural requirements must be met for an outgoing request as for conducting an investigation measure within Germany. For example, the generic investigation clause in §§ 161, 163 StPO may suffice for requesting some technical background information from foreign service providers, but the requirements of § 100j [1] StPO must be met if German authorities ask foreign service providers to voluntarily disclose subscriber data.

Little is known, however, about the scope and extent of such voluntary and unmediated cooperation between German LEAs and foreign service providers. Generally, it does not seem to be the measure of choice for German LEAs, as such requests depend on the willingness of the provider, the legality of a data transfer from the viewpoint of the provider, and as the borderline to infringe foreign sovereignty rights is narrow. Yet, there seems to be one highly important exception: a (confidential) 'General Permission Letter' by the US Department of Justice seems to allow German LEAs to get into unmediated contact with US service providers and ask them for the voluntary disclosure of traffic and subscriber data in accordance with US data protection laws.⁷²

11.4.3 Cooperation of National Service Providers with Foreign LEAs

In the opposite direction, German service providers are severely limited in any form of unmediated cooperation with foreign LEAs, including those from other EU member states. While they may voluntarily disclose technical information, any transfer of personal data requires a sufficient legal basis (Article 6 [1] GDPR). Telecommunications data is furthermore protected by § 3 TTDSG, and any unlawful disclosure in violation of the secrecy of telecommunications may even constitute a criminal offence (§ 206 StGB). Whether a data transfer or a breach of the secrecy of telecommunications is lawful depends on applicable German (or EU) law; the lawfulness of a request according to foreign criminal procedure is irrelevant. Only exceptionally, a breach of the secrecy of telecommunications may be justified on grounds of necessity (§ 34 StGB) in cases where the requested data is required to avert imminent dangers to the life or limb of a person.

⁷¹ Compare with German Federal Court of Justice, Order of 2 March 2022, 5 StR 457/21, mn. 33.

⁷² Christoph Burchard, 'Vor § 1 IRG', in Heinrich Grützner and Paul-Günter Pötz (founders), *Internationaler Rechtshilfeverkehr in Strafsachen*, 136th supplement (Heidelberg: C. F. Müller, 2024), mn. 38; Christoph Burchard, 'Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 1' (2018) *Zeitschrift für Internationale Strafrechtsdogmatik* 190–203 at 202.

Therefore, foreign LEAs are regularly required to request MLA from German authorities, including by means of an EIO. If German authorities decide, on the basis of the IRG and other applicable laws, to execute such a request, German service providers are bound by the German decision, and the same enforcement mechanisms exist as in a comparable domestic situation.

11.4.4 Opportunities and Challenges Created by the e-Evidence Regulation

The European Commission's Proposals on e-Evidence have stirred an intense debate also in Germany.⁷³ The opportunities of such a mechanism for direct and mandatory cross-border cooperation for German LEAs are evident, as they would be given less cumbersome tools to quickly access data they require for criminal investigations, compared to the current need to employ EIOs or MLA requests. Yet, strikingly, Germany has adopted a *lex loci solutionis* approach in Germany's own telecommunication, telemedia and social network legislation – the same approach as suggested in the e-Evidence Proposal and now enacted in Article 2 [1] of the e-Evidence Regulation (EU) 2023/1543.⁷⁴ In comparison to Germany's existing framework to collecting data from domestic service providers, the threshold for clandestine requests for content data is lower in the Regulation, as are the protections offered to affected parties for clandestine requests.

For service providers, the e-Evidence Regulation improves legal clarity, as the legal framework of how to deal with cross-border requests has become more precise in comparison to the previous, voluntary practice. Yet, they voiced concerns about whether they are in a position not only to assess the formal validity of a European Production or Preservation Order, but also to evaluate whether such an order is manifestly incompatible with the guarantees enshrined in the Charter of Fundamental Rights of the European Union, as the Commission proposal had suggested.⁷⁵

More generally speaking, severe doubts about the lawfulness and appropriateness of the proposals were raised. Besides questioning a sufficient basis in the Treaties – is it actually in line with the concept of 'mutual recognition' if the default action (the service provider fulfilling the request) does not involve an authority in the executing state 'recognising' a judicial decision issued by another member state?⁷⁶ – the major criticism relates to whether there are sufficient protections in the 'executing state' for the affected users. Building upon Germany's jurisprudence on the European Arrest Warrant⁷⁷ and the jurisprudence of the European Court of

⁷³ See, in particular, Martin Böse, *An Assessment of the Commission's Proposals on Electronic Evidence* (Brussels: European Parliament, 2018), [www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2018\)604989](http://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2018)604989); Burchard, 'Zugriff auf Clouddaten – Teil 1', 190; Christoph Burchard, 'Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 2' (2018) *Zeitschrift für Internationale Strafrechtsdogmatik* 249; Christoph Burchard, 'Europäische E-Evidence-Verordnung' (2019) *Zeitschrift für Rechtspolitik* 164; Robert Esser, 'Grenzüberschreitende Ermittlungen innerhalb der EU: neuer Rechtsrahmen für E-Evidence' (2019) *Strafverteidiger-Forum* 404; Elisabeth Niekrenz, 'E-Evidence-Verordnung: Datenzugriff durch Strafverfolgungsbehörden aus dem Ausland?' (2020) *Datenschutz und Datensicherheit* 535; Stefanie Schott, 'Außer Kontrolle geraten – Die E-Evidence-Vorschläge der Kommission' (2020) 1 *Strafverteidiger* I (editorial).

⁷⁴ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191/118 (e-Evidence Regulation).

⁷⁵ On the problem of privatising (parts of) criminal justice to internet service providers, see Stanislaw Tosza, 'Internet Service Providers as Law Enforcers and Adjudicators: A Public Role of Private Actors' (2021) 43 *Computer Law & Security Review* 105614.

⁷⁶ Burchard, 'Zugriff auf Clouddaten – Teil 2', 261–263.

⁷⁷ German Federal Constitutional Court, Judgment of 18 July 2005, 2 BvR 2236/04; German Federal Constitutional Court, Decision of 15 December 2015, 2 BvR 2735/14.

Human Rights,⁷⁸ there is a requirement that Germany provides at least some ‘residual’ protection in relation to data stored in Germany, requested by and then transferred to foreign LEAs – in particular, if it is data people residing in Germany have stored domestically *on purpose*. It is highly doubtful whether such ‘residual’ protection can sufficiently be provided by service providers on behalf of German authorities, as suggested in the Commission proposal. Instead, some sort of notification of German authorities – and sufficient ability to react to such a notification – seems to be required, similar to what is provided for in Article 31 Directive 2014/41/EU regarding the EIO in criminal matters. The EU legislator has also taken up this viewpoint and has enacted a mechanism to notify an authority in the requested state that may intervene in the obtaining of data (Articles 8 and 12 Regulation (EU) 2023/1543).

While the trilogue on the Commission proposals was still proceeding very slowly, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (ETS No. 224) had already been tabled for signature on 12 May 2022.⁷⁹ Two provisions at its core – Articles 6 and 7 – relate to direct, cross-border cooperation between LEAs and service providers, yet are limited to domain name registration data (Article 6), which used to be widely available before the GDPR entered into force, and subscriber information (Article 7) as defined in Article 18 of the Convention on Cybercrime. Once ratified and implemented, this would provide a legal basis for (German) service providers to disclose the requested data to foreign authorities; yet, Germany – same as all EU member states⁸⁰ – will likely require a ‘simultaneous notification of the order’, and allow its authorities to ‘instruct the service provider not to disclose the subscriber information if (i) disclosure may prejudice criminal investigations or proceedings in that Party; or (ii) conditions or grounds for refusal would apply under Article 25, paragraph 4, and Article 27, paragraph 4, of the Convention had the subscriber information been sought through mutual assistance’ (Article 7 [5] lit. c). This indeed may be seen as a blueprint for the solution found for the e-Evidence Regulation, and has been extended there also to requests for traffic and content data – which remain, within the domain of the Second Additional Protocol, a matter for (expedited) MLA (Articles 8 and 9).

⁷⁸ See *Stojkovic v. France and Belgium*, Appl. No. 25303/08, 27 October 2011, §§ 41, 55 ff.

⁷⁹ On this protocol, see Filippo Spiezia, ‘International Cooperation and Protection of Victims in Cyberspace: Welcoming Protocol II to the Budapest Convention on Cybercrime’ (2022) 23 *ERA Forum* 101.

⁸⁰ See Council Decision (EU) 2022/722 of 5 April 2022 authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, [2022] OJ L 134, 11 May 2022, p. 15, and, in particular, the declaration pursuant to Article 7 [5] [a] (p. 18).

Accessing Digital Evidence in Criminal Matters

An Inadequate Irish Legal Framework

*T. J. McIntyre and Maria Helen Murphy**

12.1 INTRODUCTION

Ireland has become the location of the European headquarters and data centres of many of the world's largest internet firms, making it a key jurisdiction for police access to data held by various providers.¹ This was highlighted by the *Microsoft Ireland* litigation, which considered whether a United States court could require the production of data held in Ireland and saw the Irish government file an unprecedented amicus brief before the US Supreme Court asserting that the Ireland–US Mutual Legal Assistance Treaty (MLAT) should be used instead.²

Yet despite the importance of this sector to the Irish economy, there is little legislation in Ireland which deals with cross-border access to data or indeed access to data generally. Ireland has failed to ratify the Cybercrime Convention; it has opted out of the European Investigation Order (EIO); and the law on interception of communications predates the modern internet and remains largely unchanged since 1993.³ For the most part, Irish practice in this area relies on older laws that are often ill-suited to digital material, with little case law to provide further guidance.

The one area where there has been modern legislation – telecoms data retention – was thrown into disarray by the April 2022 Court of Justice of the European Union (CJEU) judgment in the *Dwyer* litigation holding that the Communications (Retention of Data) Act 2011⁴ was contrary to the ePrivacy Directive.⁵ Legislation amending the 2011 Act⁶ was controversially⁷ rushed through in July 2022, but there remain significant question marks about the legality of the revised data retention regime.

* For their very helpful comments we thank Ronan Lupton, Denis Kelleher and another legal expert who has asserted their right to be forgotten. All errors are our own.

¹ The term 'provider' is used in this chapter as a catch-all covering the full gamut of internet services, including connectivity providers, webmail and messaging providers, hosting providers, domain name registrars, search engines, online gaming services and information society services generally.

² For context, see, e.g., Jennifer Daskal, 'Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0' (2018) 71 *Stanford Law Review Online* 9.

³ See, e.g., the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993.

⁴ Generally referred to in this chapter as 'the 2011 Act'. References to the 2011 Act are to the Act as amended most recently by the Communications (Retention of Data) (Amendment) Act 2022, the Criminal Justice (Miscellaneous Provisions) Act 2023 and the Policing, Security and Community Safety Act 2024.

⁵ Case C-140/20, *G.D. v. Commissioner of An Garda Síochána and others* [2022] ECLI:EU:C:2022:258.

⁶ Communications (Retention of Data) (Amendment) Act 2022.

⁷ Karlin Lillington, 'Ireland's Slapdash Approach to Data Retention Legislation Sinks to New Low', *Irish Times*, 7 July 2022, www.irishtimes.com/technology/2022/07/07/irelands-slapdash-approach-to-data-retention-legislation-sinks-to-new-low/.

This rickety legal framework is further weakened by reliance on voluntary disclosure of user data – where providers disclose data to police without any obligation to do so and without any specific legal framework regulating such requests.⁸ In particular, Ireland – apparently uniquely among EU member states – permits providers to make voluntary disclosure of user data to foreign law enforcement.⁹ The result is that there is little transparency as to how the Irish state and firms with an Irish presence handle requests for data, and in many cases there is a lack of fundamental rights safeguards against abuse.

In this chapter we consider these issues by discussing the ways in which Irish law regulates access to data for the purposes of criminal investigations, the cross-border arrangements in this area and the implications for effective law enforcement and fundamental rights.¹⁰

12.2 SETTING THE SCENE

12.2.1 *Collection of Digital Evidence*

To understand the Irish approach to the collection of digital evidence we must start with the fact that there is no general framework regulating access to data. The only technology-specific rules are those relating to interception of communications and data retention, under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 and the Communications (Retention of Data) Act 2011, respectively. However, these apply only to messages transmitted by traditional operators such as landline, cable and mobile phone providers and internet connectivity providers.¹¹

These Acts do not address over-the-top services such as WhatsApp, iMessage, or Snapchat, or search engines, social media providers, or other information society services and there is no Irish law specifically permitting access to data held by these types of providers. Consequently, it is important to bear in mind throughout this chapter that all references to ‘interception of communications’ and ‘data retention’ refer to laws that are limited to traditional telecommunications providers.

Apart from interception and data retention, Ireland does not have technology-specific rules and instead relies on the general law regarding search warrants and court orders to produce or give access to information (‘production orders’).¹² However, these powers are not consolidated in

⁸ The nature and limits of this voluntary cooperation are considered in Section 12.4 in this chapter and in more detail in T. J. McIntyre, ‘Voluntary Disclosure of Data to Law Enforcement: The Curious Case of US Internet Firms, Their Irish Subsidiaries and European Legal Standards’, in Federico Fabbrini, Edoardo Celeste and John Quinn (eds.), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Oxford: Hart, 2021).

⁹ See, e.g., Commission of the European Communities, *Non-paper: Progress Report Following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace*, 15072/16, 2 December 2016, 1, 3–4, <http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf>.

¹⁰ Two limitations should be noted. First, because this chapter focuses on the internet, we do not attempt to cover other sector-specific rules such as the exchange of information about financial transactions for criminal investigation purposes (regulated in part 2 of the Criminal Justice (Mutual Assistance) Act 2008). Second, the chapter considers access to data for the purposes of the criminal law – disclosures for national security purposes and emergency disclosures to safeguard lives are outside our scope.

¹¹ That is, ‘authorised undertakings’ as defined in the European Communities (Electronic Communications Networks and Services) (Authorisation) Regulations 2003 (SI 306 of 2003) and ‘service providers’ as defined in section 1 of the Communications (Retention of Data) Act 2011.

¹² Note that production orders are orders to produce documents or information already in being: a production order cannot be used to create an obligation to obtain new information.

one place but are spread across a range of statutes and common law rules.¹³ As Walsh puts it, ‘current statutory powers to issue search warrants constitute an unwieldy collection of disparate provisions which have been developed in a piecemeal fashion over the past two centuries. Each authorises the issue of a search warrant only when its own peculiar requirements have been satisfied.’¹⁴ The effect is that there are a range of rules regarding search warrants and production orders, depending on the type of crime being investigated, with differences such as:

- who can apply for a search warrant or production order;
- what offences can be investigated using a particular type of warrant/order;
- the evidential criteria to be met for the grant of a warrant/order;
- whether a person executing a warrant/order can require disclosure of a password necessary to operate a computer; and
- whether a person executing a warrant/order can require that information be decrypted.¹⁵

Recent pieces of legislation generally include specific provisions regarding the seizure of data. For example, section 7 of the Criminal Justice (Offences Relating to Information Systems) Act 2017 provides that search warrants issued under that Act include powers to seize computers and records, to operate computers at the place being searched, to require disclosure of passwords or encryption keys from a person at the place being searched and to require information stored on a computer to be produced in a visible and legible form.

However, older statutory powers of search and seizure do not have any similar provisions. For example, section 10 of the Criminal Justice (Miscellaneous Provisions) Act 1997¹⁶ creates a catch-all power to issue search warrants in relation to any arrestable offence and is therefore one of the most used provisions.¹⁷ But it is silent in relation to data. As a result, while a garda (police officer) carrying out a search under a section 10 warrant would be able to seize a computer and files, he or she would not be able to compel a person to reveal a password or to decrypt encrypted data.¹⁸

This reliance on the general law also means that (outside the areas of interception and data retention) there is no statutory power to compel providers to generate or log specific pieces of information. The search warrant and production order powers are static rather than dynamic – they are restricted to material which the provider already has and cannot be used to compel the provider to collect information on an ongoing basis.

The 2023 decision of the Supreme Court in *People (DPP) v. Patrick Quirke*¹⁹ has highlighted the issues resulting from the lack of a specific legal regime regarding access to digital evidence. Quirke was convicted of murder based on circumstantial evidence which included evidence of internet searches on the decomposition of human remains found on a computer hard drive. In applying for a search warrant of his home, An Garda Síochána (the police force) failed to mention their intention to seize and examine his computer. As a result, the intention to search

¹³ Maeve McDonagh and Micheál O’Dowd, *Cyber Law in Ireland* (Alphen aan den Rijn: Wolters Kluwer Law & Business, 2015), 384.

¹⁴ Dermot Walsh, *Criminal Procedure* (Dublin: Thomson Round Hall, 2002), para. 8–09.

¹⁵ For a general discussion of these differences, see, e.g., Law Reform Commission, *Report on Search Warrants and Bench Warrants* (Dublin, 2015), 47–74, www.lawreform.ie/_fileupload/Reports/Report%20on%20Search%20Warrants%20and%20Bench%20Warrants%201%20December%202015%20-%20Final%20Version.pdf.

¹⁶ As amended by section 6 of the Criminal Justice Act 2006.

¹⁷ ‘Arrestable offence’ is defined as an offence punishable by imprisonment of at least five years on conviction.

¹⁸ It has been argued that this creates a gap in relation to crimes against children in particular. See, e.g., Geoffrey Shannon, ‘Recommended Legislative Reforms on Child Protection’, *ACJRD 19th Annual Conference: Cybercrime*, 7 October 2016, https://acjrd.ie/images/PDFs/annual-conference/19th_Annual_ACJRD_Conference_Report_Cybercrime.pdf.

¹⁹ *DPP v. Patrick Quirke* [2023] IESC 5.

the ‘digital space apart from the physical space’ was not put before the judge issuing the search warrant. The Supreme Court found that the search of digital devices was a particularly serious intrusion on privacy which required judicial analysis²⁰ of the proportionality of that search. The Supreme Court held that while the legislation permitted digital searches, the intention to seize and search digital devices must be brought to the attention of the judge issuing the search warrant if a search is to be lawful.²¹ This meant that the search and seizure of *Quirke*’s devices had been unlawful. However, in a subsequent decision as to the consequences of the ruling, the Supreme Court held that the police force had acted in good faith and could not have been expected to anticipate the novel legal finding regarding digital-space privacy in the principal *Quirke* ruling.²² Consequently, the mistake in the search warrant application was found to be owing to ‘honest inadvertence’ and the criminal conviction was affirmed.²³

12.2.2 Admissibility of Digital Evidence

Irish law takes a technology-neutral approach towards digital evidence by providing that the rules of evidence shall not exclude electronic evidence ‘on the sole ground that it is an electronic communication, an electronic form of a document, an electronic contract, or writing in electronic form’.²⁴ As McGrath notes, Irish courts ‘have not recognised electronic evidence as a distinct category of evidence requiring separate consideration or safeguards’ and instead treat such evidence ‘simply as a variety of documentary evidence, or sometimes as real evidence’.²⁵ Problems such as what constitutes the ‘original’ of a document produced on a computer have been addressed within that framework.²⁶ Digital evidence is also included within the documentary evidence system established by the Criminal Evidence Act 1992, which limits the hearsay rule and provides more lenient standards for the admissibility of business records.

Despite being admissible in principle, digital evidence presents problems in practice. Several cases have set a high threshold before digital evidence can be used. In *People (DPP) v. Meehan*,²⁷ the Court of Criminal Appeal summarised the position as follows: ‘[B]efore the judge can decide whether computer printouts are admissible, whether as real evidence or as hearsay, it is necessary to call appropriate authoritative evidence to describe the function and operation of the computer.’ This requirement for ‘appropriate authoritative evidence to describe the function and operation of the computer’ proved difficult to meet when evidence was received from foreign service providers. In practice, it meant that detailed evidence was required from specialists in the relevant providers as to how their systems operated.²⁸ Some providers were willing to provide this additional evidence, but others were not, creating difficulties for prosecutors.²⁹

²⁰ In accordance with *Damache v. DPP* [2012] IESC 11.

²¹ *DPP v. Patrick Quirke* [2023] IESC 5.

²² *DPP v. Patrick Quirke* [2023] IESC 20.

²³ This applied *DPP v. JC* [2017] 1 IR 417, a 2017 Supreme Court decision which overruled the previous legal position on unconstitutionally obtained evidence in Ireland.

²⁴ Electronic Commerce Act 2000, s. 22.

²⁵ Declan McGrath, *Evidence*, 2nd ed. (Dublin: Round Hall, 2014), 910. See, e.g., *DPP v. McD* [2016] IESC 71.

²⁶ McGrath, *Evidence*, 910.

²⁷ *DPP v. Brian Meehan* [2006] IECCA 104, relying on *R. v. Cochrane* (1993) Crim. LR 48.

²⁸ Michael Brady, ‘Cyber-Crime, Confiscation, Disclosure, Mutual Legal Assistance and the Budapest Convention 2001, and Privacy Law In Ireland’, *Fighting Cybercrime: Between Legal Challenges and Practical Difficulties*, 10–11 May 2016, 20–21, www.isrcl.com/wp-content/uploads/2021/05/Brady-Michael-Cyber-crime-confiscation-disclosure-mutual-legal-assistance-the-Budapest-Convention-2001-and-Privacy-law-in-Ireland.pdf.

²⁹ *Ibid.*

This issue has been partially mitigated in relation to evidence from the USA. In September 2014 the Irish and US authorities agreed a revised form of certificate under the Ireland–US MLAT, which certifies the ‘function and operation of the system’ in relation to evidence which is automatically generated.³⁰ In *People (DPP) v. Moran*,³¹ the Court of Appeal accepted that Facebook records of messages between users were admissible based on this certificate, without any further evidence being required. This makes the task of Irish prosecutors significantly easier in relation to evidence from the USA, but leaves the same issue in relation to evidence from elsewhere.³²

12.2.3 Data Retention Obligations

12.2.3.1 Background

Irish data retention law has changed significantly in recent years. The law in this area is contained in the Communications (Retention of Data) Act 2011, which, as originally adopted, was a largely verbatim transposition of the Data Retention Directive³³ into Irish law.³⁴ However, it was clear after the 2014 judgment in *Digital Rights Ireland*³⁵ and the 2016 judgment in *Tele2*³⁶ that the 2011 Act failed to meet the standards of the Charter of Fundamental Rights and the European Convention on Human Rights (ECHR). In a 2017 report commissioned by the Department of Justice and Equality to review the law on data retention, the former Chief Justice, John Murray, found that

the central finding in *Tele2* is clear: legislation providing for a system of general and indiscriminate communications data retention without exception is precluded by Article 15(1) of Directive 2002/58/EC. By the same token ... it is also clear that the blanket data retention measures imposed by the Communications (Retention of Data) Act, 2011 are in essence indistinguishable from those impugned in *Tele2*.³⁷

In that report, Murray also identified numerous other problems:

The *principal* frailties of the 2011 Act ... include: allowing statutory bodies an effective power of self-certification when making disclosure requests; failure to provide for prior independent authorisation of disclosure requests; failure to adhere to the clear statement principle by

³⁰ Ibid.

³¹ *People (DPP) v. Moran* [2018] IECA 176.

³² Though note the 2016 Supreme Court decision in *DPP v. McD* [2016] IESC 71, which suggests that the Irish courts may in the future reconsider the requirement for ‘appropriate authoritative evidence’ regarding digital evidence. In that case, the court held that there was no need for such evidence in relation to closed-circuit television (CCTV) footage, even when digitally recorded, as ‘such devices have become ubiquitous in everyday life and their essential purpose and operation would be readily apparent to any reasonable person’ (para. 55). The judgment also states that ‘it may well be to over-read [*R. v. Cochrane*] even to say that it applies to all computers’ (para. 54).

³³ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

³⁴ For the Irish law prior to 2011, see T. J. McIntyre, ‘Data Retention in Ireland: Privacy, Policy and Proportionality’ (2008) 24(4) *Computer Law & Security Report* 326.

³⁵ Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and others* [2014] ECLI:EU:C:2014:238.

³⁶ Joined Cases C-203/15 and C-698/15, *Tele2 Sverige and others* [2018] ECLI:EU:C:2016:970.

³⁷ John Murray, *Review of the Law on the Retention of and Access to Communications Data* (Dublin: Department of Justice and Equality, 2017), 44–45, www.justice.ie/en/JELR/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf/Files/Review_of_the_Law_on_Retention_of_and_Access_to_Communications_Data.pdf; see also Data Protection Commissioner, *An Garda Síochána: Final Report of Audit* (March 2014), www.digitalrights.ie/wp-content/uploads/2014/07/Garda-data-protection-audit.pdf.

permitting undue legislative scatter of the rules governing data retention and disclosure; failure to articulate sufficiently clear objective criteria governing the conditions, circumstances and purposes surrounding data retention and disclosure; failure to provide clear procedures and protocols for the statutory bodies given a right of access to retained data; failure to make provision for the notification of persons affected, either directly or indirectly, by disclosure requests; failure to make appropriate provision for a remedy for wrongful access to retained data; failure to provide for the storage of retained data within the European Union.³⁸

Despite this, official acknowledgement of the need for reform did not come until October 2017 when the Department of Justice and Equality published draft legislation to replace the 2011 Act.³⁹ However, that proposal itself still failed to meet the criteria set out in *Tele2* and was heavily criticised in pre-legislative scrutiny by the Oireachtas Joint Committee on Justice and Equality.⁴⁰

In the meantime, the Irish state persisted with the use of data retention under the 2011 Act until finally forced to act by the CJEU judgment in *G.D. v. Commissioner of An Garda Síochána and others*⁴¹ (better known in Ireland as the *Dwyer* case), which confirmed that the key elements of the 2011 Act were contrary to EU law. That judgment prompted the Irish government to push the Communications (Retention of Data) (Amendment) Act 2022 through Parliament in July 2022 as an emergency response with just four days of debate. This was extremely controversial; incredibly for a measure providing for mass surveillance, there was no public consultation, no prior consultation with the Data Protection Commission⁴² and no data protection impact assessment, and Members of Parliament were not provided with the text in advance. This sudden exigency, long after Irish law was known to be in breach of EU law, is difficult to see as anything other than ‘manufactured urgency in an attempt to sandbag any proper democratic scrutiny’.⁴³

This manufactured urgency may have backfired on the state by making the 2022 Act unenforceable. Ireland failed to notify a draft of the 2022 Act to the European Commission⁴⁴ as required by the Technical Regulations Information System (TRIS) procedure,⁴⁵ with the result that the legislation will almost certainly be found invalid if challenged.⁴⁶ The state has attempted to mend its hand by a retrospective notification of the Act to the Commission under TRIS ‘on

³⁸ Murray, *Review of the Law*, 115 (emphasis added).

³⁹ Department of Justice and Equality, *General Scheme of the Communications (Retention of Data) Bill 2017*, 3 October 2017, [www.justice.ie/en/JELR/General_Scheme_-_Communications_\(Retention_of_Data\)_Bill.pdf/Files/General_Scheme_-_Communications_\(Retention_of_Data\)_Bill.pdf](http://www.justice.ie/en/JELR/General_Scheme_-_Communications_(Retention_of_Data)_Bill.pdf/Files/General_Scheme_-_Communications_(Retention_of_Data)_Bill.pdf).

⁴⁰ Joint Committee on Justice and Equality, *Report on Pre-legislative Scrutiny of the Communications (Retention of Data) Bill 2017*, 32/JAE/22, January 2018, www.oireachtas.ie/parliament/media/committees/justice/2018/Data-Retention-Report-Final.pdf.

⁴¹ *G.D. v. Commissioner of An Garda Síochána and others*.

⁴² As required by the General Data Protection Regulation (GDPR) and the Law Enforcement Directive. See, e.g., section 84(12) of the Data Protection Act 2018 and Article 36(4) of the Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016, [2016] OJ L 119/1, 4 May 2016.

⁴³ Cormac McQuinn, ‘Concern at “Rushed” Nature of Proposed Law to Deal With Fallout from Dwyer Appeal on Data’, *Irish Times*, 30 June 2022, www.irishtimes.com/politics/oireachtas/2022/06/30/concern-at-rushed-nature-of-proposed-law-to-deal-with-fallout-from-dwyer-appeal-on-data/.

⁴⁴ Cianan Brennan, ‘“Illegitimate” Data Law Still Stands as EU Was Not Notified of New Act Rushed Through This Year’, *Irish Examiner*, 4 December 2022, www.irishexaminer.com/news/arid-41021237.html.

⁴⁵ See Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on information society services (codification), [2015] OJ L 241/1, 9 September 2015.

⁴⁶ Case C-194/94, *CIA Security International SA v. Signalson SA and Securitel SPRL* ECLI:EU:C:1996:172.

a strictly precautionary and without prejudice basis’.⁴⁷ However, it is clear that only *draft* legislation may be notified under TRIS, making this belated notification of no legal effect.

The 2022 Act is, broadly speaking, a minimal response to the judgment in *G.D. v. Commissioner of An Garda Síochána and others*.⁴⁸ As discussed later, it maintains general and indiscriminate retention of traffic data and location data, addressing the CJEU jurisprudence by limiting the use of that retained data to state security purposes. It provides for general and indiscriminate retention of user data and internet source data for both state security and criminal law purposes. It also introduces, for the first time in Irish law, a preservation order (quick freeze) system in relation to telecommunications data. While in some regards the 2022 Act is an improvement over the 2011 Act, it nevertheless fails to address the majority of the recommendations in the Murray report and almost certainly fails to meet the standards articulated by the CJEU and the European Court of Human Rights (ECtHR) in relation to state surveillance. For example, the Act does not define what is meant by ‘security of the state’, does not provide explicit protection for journalists’ sources and does not provide any judicial remedy to individuals for breaches.⁴⁹ It also fails to address concerns about the adequacy of the designated judge and complaints referee oversight mechanisms, which are discussed further in Section 12.4.5 of this chapter.

12.2.3.2 Legal Framework

The Communications (Retention of Data) Act 2011, as now amended by the Communications (Retention of Data) (Amendment) Act 2022,⁵⁰ applies only to ‘service providers’, defined as persons ‘engaged in the provision of a publicly available electronic communications service or a public communications network by means of fixed line or mobile telephones or the Internet’.⁵¹ The 2011 Act therefore covers traditional telecommunications providers only and does not apply to other services such as search engines, private networks, or over-the-top communications services such as WhatsApp or iMessage. There are no general data retention obligations in Irish law for those other services.

All service providers must retain ‘user data’, defined in section 1 of the Act to mean name, address, mobile phone number or fixed telephony phone number, international mobile subscriber identity (IMSI), international mobile equipment identity (IMEI), internet protocol (IP) address allocated by the service provider to the communication, user identity (ID), date and time of initial activation of service and date and time of last outgoing telephony communication.⁵² This data must be retained on all users for one year.⁵³ Note, however, that the 2011 Act does not require registration for services such as prepaid subscriber identity module (SIM) cards – the obligation is to retain data already processed, not to process additional data, and services can still be provided anonymously.

All service providers must also retain ‘internet source data’, defined in section 1 of the Act to mean ‘the IP address, whether dynamic or static, allocated by the service provider to the source of

⁴⁷ Notification number 2022/872/IRL.

⁴⁸ *G.D. v. Commissioner of An Garda Síochána and others*.

⁴⁹ See, e.g., Irish Council of Civil Liberties, ‘Why the Data Retention Bill Is So Problematic’, 6 July 2022, www.iccl.ie/2022/why-the-data-retention-bill-is-so-problematic/.

⁵⁰ Also note section 78 of the Criminal Justice (Miscellaneous Provisions) Act 2023, which addresses numerous drafting errors in the Communications (Retention of Data) (Amendment) Act 2022. Further changes are also made by the Policing, Security and Community Safety Act 2024.

⁵¹ Communications (Retention of Data) Act 2011, s. 1.

⁵² *Ibid.*, s. 3.

⁵³ The Minister for Justice may vary this period: Communications (Retention of Data) Act 2011, s. 3(2).

a communication [and] the name and address of the subscriber or registered user to whom an IP address was allocated at the time of the communication'.⁵⁴ This data must be retained on all users for one year.⁵⁵

Retention of 'Schedule 2 data' – broadly speaking, the wider set of communications traffic data and location data – is regulated by section 3A. This permits the Minister for Justice to apply to a High Court judge *ex parte* (that is, in a closed hearing) for an order providing for general and indiscriminate retention of Schedule 2 data for twelve months. The judge may grant such an order if satisfied that it is necessary and proportionate for safeguarding the security of the state.⁵⁶ Where such an order is made, it applies to all service providers in respect of all users.⁵⁷ Such an order was made on 26 June 2023, to remain in force for one year. However, the order under section 3A may be renewed, and the assumption must be that there is an intention to keep this data retention in place indefinitely through rolling annual renewals.

12.2.3.3 Access to Data

User data can be accessed by An Garda Síochána, the Defence Forces, the Revenue Commissioners and the Garda Síochána Ombudsman Commission (police disciplinary body).⁵⁸ Depending on the investigating body, user data may be accessed for the purpose of investigating an offence (not necessarily a serious offence) or a revenue offence, for national security purposes, for police disciplinary matters, for protecting the life or personal safety of a person or for determining the whereabouts of a missing person. A requirement to disclose user data is on the basis of internal authorisation by a senior official within each body – there is no requirement for authorisation by a judge or independent body.⁵⁹ There is no proportionality test in relation to disclosure of user data.

Internet source data can be accessed by An Garda Síochána, the Defence Forces, the Revenue Commissioners and the Garda Síochána Ombudsman Commission.⁶⁰ Depending on the investigating body, user data may be accessed for the purpose of investigating a serious offence or a revenue offence, for national security purposes, for police disciplinary matters, for protecting the life or personal safety of a person or for determining the whereabouts of a missing person. Authorisation to require disclosure of internet source data is granted by a District Court judge, applying a test of necessity and proportionality.⁶¹ However, in cases of urgency these bodies can access internet source data on the basis of internal authorisation by a senior official, followed by an application to a District Court judge for retrospective approval.⁶²

⁵⁴ Communications (Retention of Data) Act 2011, s. 3B. Note that this overlaps with the definition of 'user data'.

⁵⁵ The Minister for Justice may vary this period: Communications (Retention of Data) Act 2011, s. 3B(2).

⁵⁶ *Ibid.*, s. 3A(4).

⁵⁷ *Ibid.*, s. 3A(5).

⁵⁸ Section 6 of the Communications (Retention of Data) Act 2011 as applied by section 98 of the Garda Síochána Act 2005. The Data Protection Commission can also authorise access (section 5). Service providers are prohibited from accessing data retained under the Act except where it is accessed: (a) at the request and with the consent of a person to whom the data relates, (b) for the purpose of complying with a disclosure request, (c) in accordance with a court order or (d) as may be authorised by the Data Protection Commissioner. The Act also provides for the extension of this and other powers to the Competition and Consumer Protection Commission in relation to competition offences, but at the time of writing these provisions have not yet been brought into force.

⁵⁹ Communications (Retention of Data) Act 2011, s. 6.

⁶⁰ *Ibid.*, s. 6C as applied by s. 98 of the Garda Síochána Act 2005.

⁶¹ Communications (Retention of Data) Act 2011, s. 6C(6).

⁶² *Ibid.*, s. 6D.

Schedule 2 data can be accessed by An Garda Síochána and the Defence Forces for the purpose of state security.⁶³ Authorisation to require disclosure of Schedule 2 data is granted by a District Court judge, applying a test of necessity and proportionality.⁶⁴ However, in cases of urgency these bodies can access Schedule 2 data on the basis of internal authorisation by a senior official, followed by an application to a District Court judge for retrospective approval.⁶⁵

Schedule 2 data which is being held by a service provider for a purpose other than compliance with a High Court retention order under section 3A (for example, for its own billing or quality assurance purposes) can be accessed for purposes other than national security, including investigation of serious offences and revenue offences.⁶⁶ The mechanism for doing so is a production order issued by a District Court judge on the basis of a test of necessity and proportionality.⁶⁷

*Cell site location data*⁶⁸ (in essence, the most recent geographic location of a device) can be accessed by An Garda Síochána on the basis of internal authorisation for protecting the life or personal safety of a person or for determining the whereabouts of a missing person.⁶⁹

12.2.3.4 Data Preservation

Irish law does not generally provide for data preservation (quick freeze) orders in relation to criminal investigations. However, the 2011 Act permits An Garda Síochána, the Defence Forces, the Revenue Commissioners and the Garda Síochána Ombudsman Commission to apply to a District Court judge for a preservation order in relation to Schedule 2 data.⁷⁰ This may be done for investigating a serious offence or a revenue offence, for national security purposes, for police disciplinary matters, for protecting the life or personal safety of a person or for determining the whereabouts of a missing person. Those bodies may also issue a temporary preservation order based on internal authorisation in cases of urgency.⁷¹

12.2.3.5 Voluntary Disclosures

Outside the 2011 Act, Irish police adopted a parallel tactic of obtaining telecommunications data on a voluntary basis. This practice developed in reliance on section 8 of the Data Protection Acts 1988–2003 which disapplied data protection restrictions on processing personal data where processing was ‘required for the purpose of safeguarding the security of the State’ or ‘required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders . . . [if] the application of those restrictions would be likely to prejudice [this enforcement]’.⁷² While this did not

⁶³ Ibid., s. 6A.

⁶⁴ Ibid., s. 6A(4).

⁶⁵ Ibid., s. 6B. See also sections 7C and 7D, which create overlapping powers to seek production orders in relation to Schedule 2 data that is being stored by a service provider for purposes other than compliance with a retention order under section 3A.

⁶⁶ Communications (Retention of Data) Act 2011, s. 7C.

⁶⁷ Ibid., s. 7C(8).

⁶⁸ Defined in section 6E(5) of the Communications (Retention of Data) Act 2011 to mean ‘data processed by means of an electronic communications network that identifies the most recent geographic location of the device or equipment used by a user when availing of a publicly available electronic communications service’.

⁶⁹ Communications (Retention of Data) Act 2011, s. 6E.

⁷⁰ Ibid., s. 7A, as applied by section 98 of the Garda Síochána Act 2005. There is a parallel scheme of ‘temporary production orders’ under section 7D.

⁷¹ Communications (Retention of Data) Act 2011, s. 7B.

⁷² This section has since been replaced by section 41 of the Data Protection Act 2018.

compel providers to disclose data, or provide a legal basis for police to request such data, it was nevertheless frequently used by police to obtain data for matters outside the scope of the 2011 Act, such as minor offences, sidestepping the safeguards in that legislation in a way that clearly contravened EU law and ECHR standards.⁷³ While the Murray report should have put an end to this practice, there are anecdotal reports that similar requests continue to be made. Service providers should be aware that disclosure of user data without a statutory basis is in breach of section 5 of the 2011 Act.

12.2.3.6 Notification, Redress and Judicial Oversight

Section 12G of the 2011 Act provides for notification of individuals that Schedule 2 data relating to them has been disclosed, except where the disclosure is for state security purposes. There is no provision for notification of disclosure of user data, internet source data or cell site location data. There is limited provision for investigation and redress in case of wrongful access to data by the state through a complaints referee mechanism,⁷⁴ and there is provision for oversight by a designated judge of the High Court.⁷⁵ These are considered in detail in Section 12.4.5 of this chapter.

12.3 TERMINOLOGY AND CATEGORISATIONS

12.3.1 *Data*

12.3.1.1 Terminology

There is no general definition of ‘data’ in Irish criminal procedure; the only specific references to ‘data’ appear to be in the Communications (Retention of Data) Act 2011, where ‘data’ is defined as ‘traffic data or location data and the related data necessary to identify the subscriber or user’,⁷⁶ and in the Criminal Justice (Offences Against Information Systems) Act 2017, where ‘data’ is defined as ‘any representation of facts, information or concepts in a form capable of being processed in an information system, and includes a programme capable of causing an information system to perform a function’.⁷⁷ However, those definitions apply only within the context of each Act – not more generally.

Instead, legislation dealing with search warrants, production orders and evidence generally refers to ‘documents’, ‘records’ or ‘information’, with these terms typically being defined to include computer data also. For example, section 7(4) of the Criminal Justice (Offences Relating to Information Systems) Act 2017 gives the power to issue search warrants which allow police to:

- (a) operate any computer at the place that is being searched or cause any such computer to be operated by a person accompanying the [police officer] for that purpose, and
- (b) require any person at that place who appears to the [police officer] to have lawful access to the information in any such computer—

⁷³ See, e.g., Murray, *Review of the Law*, 44–45; Data Protection Commissioner, ‘An Garda Síochána’, 61–62.

⁷⁴ Communications (Retention of Data) Act 2011, s. 10.

⁷⁵ *Ibid.*, s. 11.

⁷⁶ *Ibid.*, s. 1.

⁷⁷ Criminal Justice (Offences Against Information Systems) Act 2017, s. 1.

- (i) to give to the [police officer] any password necessary to operate it and any encryption key or code necessary to unencrypt the information accessible by the computer,
- (ii) otherwise to enable the [police officer] to examine the information accessible by the computer in a form in which the information is visible and legible, or
- (iii) to produce the information in a form in which it can be removed and in which it is, or can be made, visible and legible.⁷⁸

12.3.1.2 Categorisation

Just as there is no general definition of ‘data’ in Irish criminal procedure, there is no general classification or regulation of *types* of data. For example, there is no specific categorisation or regulation of access to unread emails, draft emails, chat rooms, communication in the context of online games, domain name registration details or machine-to-machine data.

There is a content/metadata distinction in the context of telecommunications surveillance under the interception and data retention regimes. Mandatory interception of the content of relevant telecommunications messages requires a warrant signed by the Minister for Justice under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, while police access to metadata is governed by the Communications (Retention of Data) Act 2011 and may require judicial approval, depending on the type of metadata involved and the purpose for which it is sought.⁷⁹ The Communications (Retention of Data) (Amendment) Act 2022 has recently introduced distinct categories of ‘internet source data’, ‘cell site location data’ and ‘user data’ with different rules applying to each (see Section 12.2.3).

12.3.2 What Services Are Covered? ‘Service Providers’ and ‘Authorised Undertakings’

As already noted, Irish interception and data retention laws apply only to traditional telecoms providers such as mobile phone or broadband providers. Specifically, the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 applies to messages being transmitted by ‘authorised undertakings’, while the Communications (Retention of Data) Act 2011 applies to ‘service providers’.⁸⁰ In both cases, therefore, over-the-top services and other information society services do not fall within the scope of this legislation.

⁷⁸ This power raises issues as to whether compelled disclosure of a password might violate the privilege against self-incrimination, but the Irish courts have yet to address this point. Compare Orin S. Kerr, ‘Compelled Decryption and the Privilege Against Self-Incrimination’ (2019) 97 *Texas Law Review* 767; and Caren Myers Morrison, ‘Passwords, Profiles, and the Privilege Against Self-Incrimination: Facebook and the Fifth Amendment’ (2012) 65 *Arkansas Law Review* 133. The Irish authorities have stated that ‘prosecution for withholding passwords is generally not done due to the right against self-incrimination’: Council of the European Union, *Evaluation Report on the Seventh Round of Mutual Evaluations – The Practical Implementation and Operation of European Policies on Prevention and Combating Cybercrime: Report on Ireland*, 7160/h/17, 2 May 2017, 68, <http://data.consilium.europa.eu/doc/document/ST-7160-2017-REV-1-DCL-1/en/pdf>.

⁷⁹ Section 2 of the Communications Act 2011 provides that ‘[t]his Act does not apply to the content of communications transmitted by means of fixed network telephony, mobile telephony, Internet access, Internet e-mail or Internet telephony’.

⁸⁰ ‘Authorised undertakings’ as defined in the European Communities (Electronic Communications Networks and Services) (Authorisation) Regulations 2003 (SI 306 of 2003) and ‘service providers’ as defined in section 1 of the Communications Act 2011.

In 2016 the Department of Justice and Equality announced plans to extend the interception regime to over-the-top services also. According to the policy document:

Communications services delivered over the internet are not covered by the current legislation as the powers of direction currently vested in the Minister for Communications are effectively restricted to Telecoms and Postal Service providers. This means that communications services such as those provided by the major Internet based entities cannot be made subject to the legislation. In addition, the terminology in the Act of 1993 does not adequately reflect the modern face of communications, particularly where defining ‘communications’ and communications addresses is concerned. As the legislation stands Ireland can only comply to a limited extent with requests from other EU Member States for mutual legal assistance where interception is concerned. The fact of the matter is that mobile devices are now used to communicate in a much wider array of ways than simply by texting or holding a telephone conversation. The legislation has not kept pace with these developments and needs to be changed.⁸¹

This proposal was light on detail, but essentially proposed that the existing interception framework⁸² should be extended to information society services, including search engines and social media.⁸³ However, it was clear that the plan to simply extend the existing interception regime was not credible; the legal framework for interception lacks the basic safeguards (such as independent judicial authorisation and controls on use of intercepted data) necessary to ensure compliance with the ECHR and the Charter of Fundamental Rights.⁸⁴ There have been no further public updates since this proposal was published and it appears to have stalled, possibly owing to significant pushback from the internet industry, which has demanded that any new law should provide for significant reform to include judicial authorisation of interception.⁸⁵

12.4 DOMESTIC COOPERATION BETWEEN LEAs AND SERVICE PROVIDERS

12.4.1 Introduction

Access to data held by providers has historically been extremely common in Irish criminal investigations. The main type of data accessed is that held by traditional telecoms providers: state agencies requested communications data (mobile, landline and internet) approximately 92,200 times over the period from 2013 to 2017 inclusive, roughly 18,450 times each year on average.⁸⁶ The Garda Síochána (police force) was by far the biggest user of this information at 90,200 requests, followed by the Defence Forces (1,380), the Garda Síochána Ombudsman

⁸¹ Department of Justice, ‘Policy Document on Proposed Amendments to the Legislative Basis for the Lawful Interception of Communications’.

⁸² Postal and Telecommunications Services Act 1983, s. 110.

⁸³ As defined in EC Directive 98/34/EC of the European Parliament and Council laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services, OJ L 204, 21 July 1998, p. 37, and paragraph 18 of the Preamble of Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on Electronic Commerce), OJ L 178, 17 July 2000, p. 1.

⁸⁴ See, in particular, Maria Helen Murphy, ‘The Analytical Approach of the European Court of Human Rights in Surveillance Cases: The Implications, Justifications, and Future of the Court’s Reasoning, with a Focus on the Legislative Impact in Ireland’, PhD thesis, University College Cork (2013), ch. 5.

⁸⁵ See, e.g., Wayne O’Connor, ‘New Laws to Monitor Criminal Messaging Risk Pushing Out Technology and Social Media Firms’, *Irish Independent*, 19 November 2017, www.independent.ie/irish-news/new-laws-to-monitor-criminal-messaging-risk-pushing-out-technology-and-social-media-firms-36333077.html.

⁸⁶ Cormac O’Keeffe, ‘Personal Data Shared 92,000 Times to State Agencies by Phone and Internet Firms’, *Irish Examiner*, 10 December 2018, www.irishexaminer.com/opinion/commentanalysis/arid-30890965.html.

Commission (440) and the Revenue Commissioners (150). Of the Garda requests, approximately half were for subscriber data (such as name and address of a subscriber) and half for call and internet data (such as numbers called and phone location history). However, the number of requests fell dramatically in the period between the CJEU judgment in *G.D.*⁸⁷ and the bringing into force of the Communications (Retention of Data) (Amendment) Act 2022, with just 299 Garda requests from January to May 2023.⁸⁸

Access to other forms of data is not as ubiquitous but is still common. There are no official statistics on this point, but transparency reports published by Microsoft, Facebook, Google and Twitter indicate that a total of 1,259 disclosure requests were made by state agencies over the period from 2013 to June 2018.⁸⁹ Requests to smaller and domestic providers are harder to gauge, as many do not publish transparency reports, but it is clear that the number of these requests is on the increase.⁹⁰ Transparency reports do not usually identify the legal basis for requests, but many of these appear to be requests for voluntary disclosure.⁹¹

12.4.2 *Distinction between Domestic/National and Cross-Border/Transnational Situations*

Irish law does not draw a general distinction between domestic/national and cross-border/transnational situations in relation to access to data. The rules that determine whether data can be accessed by a compulsory process depend on the legislative language creating each power.

12.4.3 *Nature of the Cooperation*

Police access to information held by providers in Ireland is based on a mix of mandatory and voluntary cooperation. In this section we consider the legal framework for mandatory cooperation (where there is a legal basis for the cooperation of providers who can be *compelled* to provide information) and voluntary cooperation (where providers cannot be *compelled* to provide information and there may or may not be an explicit legal basis *permitting* them to do so).

12.4.3.1 *Mandatory Cooperation*

There is no general legal basis for mandatory cooperation: as we outlined in Section 12.2.1, Irish law provides different rules in respect of each type of investigative measure. Consequently, the main investigative powers – interception of communications, access to retained data, search warrants and production orders – differ widely on the basic criteria: What state bodies may seek data? From what types of providers? For what purposes? In respect of what types of crime? Using what type of authorisation? These powers are outlined in Section 12.4.4.

Data obtained through mandatory cooperation is capable of being used as evidence, subject to the ordinary rules of admissibility. In practice, the Irish state has a long-standing policy against using communications intercept evidence (evidence obtained under the Interception of Postal

⁸⁷ *G.D. v. Commissioner of An Garda Síochána and others*.

⁸⁸ Cianan Brennan, 'Garda Requests for Phone Records Down Dramatically Since New Law Was Enacted', *Irish Examiner*, 15 January 2024, www.irishexaminer.com/news/courtandcrime/arid-41308759.html.

⁸⁹ Cormac O'Keeffe, '1,250 Requests to Access Private Data', *Irish Examiner*, 26 November 2018, www.irishexaminer.com/news/arid-30887779.html.

⁹⁰ See, e.g., Michele Neylon, 'Increasing Transparency', Blacknight Blog, 14 June 2018, <https://blacknight.blog/increasing-transparency.html>.

⁹¹ See, e.g., McIntyre, 'Voluntary Disclosure of Data to Law Enforcement'.

Packets and Telecommunications Messages (Regulation) Act 1993) in prosecutions, apparently to avoid revealing details of this intercept capability.⁹² It is important to note that this policy does not extend to communications which are obtained other than through the 1993 Act – for example, messages which have been obtained from a seized mobile phone are frequently used in evidence.

Any mandatory cooperation requirement can in principle be challenged either by the provider or by the individual whose data is sought. For example, in *CRH Plc, Irish Cement Ltd & others v. The Competition and Consumer Protection Commission*, one of the plaintiffs challenging a warrant that authorised search of the Irish Cement Limited premises was an executive who successfully claimed that seizure of his entire email account was disproportionate.⁹³ The admissibility of evidence obtained in this way can also be challenged by a defendant in any subsequent criminal trial, and the Irish exclusionary rule will mean that such evidence may be excluded if it was obtained illegally or unconstitutionally.⁹⁴

To challenge access to data the individual must, of course, be aware of the fact that their data has been sought. However, Irish law does not generally provide for any such notification to individuals.⁹⁵ This gap is only partly remedied by the policies of some of the major providers (such as Apple, Facebook, Microsoft and Yahoo) which commit to notifying users where their data is sought, with some exceptions.⁹⁶

The extent of the obligations imposed on providers varies as between interception, data retention and search warrants/production orders. In the case of search warrants/production orders, the obligations imposed are relatively straightforward – to cooperate with a search at a particular place, provide decryption or login information or produce certain information by a particular time.⁹⁷ In the context of data retention, providers are obliged to retain data so that it can be disclosed without delay⁹⁸ and the Minister for Justice may impose additional technical requirements in relation to data quality.⁹⁹ The position is opaque in relation to interception, where there is no public information as to the content of warrants under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 or the underlying ministerial directions these warrants rely upon, and no details as to whether there is a time limit for compliance or what other obligations might be imposed on authorised undertakings.

The format in which data must be provided varies. In relation to data retention, the Communications (Retention of Data) Act 2011 provides an extensive list of information to be retained and provided. In the case of search warrants and production orders, the statutory powers do not require provision of information in any particular format except to the extent that some powers may require decryption of information and provision of information in a form in which

⁹² Justice, *Intercept Evidence: Lifting the Ban* (London: Justice, 2006), 56–57, <https://files.justice.org.uk/wp-content/uploads/2015/07/06170838/Intercept-Evidence-1-October-2006.pdf>.

⁹³ *CRH Plc, Irish Cement Ltd & ors v. The Competition and Consumer Protection Commission* [2017] IESC 34.

⁹⁴ On the extent of this rule and judicial discretion to admit unconstitutionally obtained evidence, see Yvonne Marie Daly, ‘Overruling the Protectionist Exclusionary Rule: *DPP v JC*’ (2015) 19(4) *International Journal of Evidence & Proof* 270.

⁹⁵ Except in relation to Schedule 2 data under the Communications (Retention of Data) Act 2011.

⁹⁶ The T-CY Cloud Evidence Group, *Criminal Justice Access to Data in the Cloud: Cooperation with ‘Foreign’ Service Providers* (Strasbourg: Council of Europe, 3 May 2016), s. 2.2.5, <https://rm.coe.int/168064b77d>.

⁹⁷ In practice, seven days seems to be the norm for compliance with a search warrant or production order. See, e.g., US Supreme Court, *United States of America v. Microsoft Corporation on Writ of Certiorari to the United States Court of Appeals for the Second Circuit, Joint Appendix* (2017), 37, www.supremecourt.gov/DocketPDF/17/17-2/22918/20171206204555098_United%20States%20v.%20Microsoft%20Joint%20Appendix.pdf.

⁹⁸ Communications (Retention of Data) Act 2011, s. 12D(a).

⁹⁹ *Ibid.*, s. 12F(2)(a).

the ‘information is visible and legible’. In relation to intercept material, it may be that ministerial warrants and directions to telecommunications providers prescribe the format in which data is to be provided, but there is no public information as to the content of these directions.

Failure to comply with an interception warrant, search warrant, production order, retention obligation or disclosure requirement will constitute an offence, subject in some cases to defences of reasonable excuse or due diligence.¹⁰⁰ These statutory powers do not define these defences further and it is not clear whether the defences would include reasons such as conflicting legal obligations or excessive costs of compliance.¹⁰¹

12.4.3.2 Voluntary Cooperation

In addition to mandatory disclosure, Irish police rely on voluntary cooperation by providers.¹⁰² We have already seen this in the context of data retention (in Section 12.2.3), where there is a questionable practice of seeking telecommunications data in situations where disclosure would not be permitted under the Communications (Retention of Data) Act 2011.¹⁰³ Requests for voluntary disclosure can be used for other data also if providers are willing to cooperate – for example, Ireland’s leading domestic hosting provider and domain name registrar states in its law enforcement guidelines that it will provide user information on the basis of ‘a valid request signed by a Garda Superintendent or higher rank’.¹⁰⁴

12.4.3.3 Historical Development of Voluntary Disclosure

Voluntary disclosure initially developed on the basis of section 8 of the Data Protection Acts 1988 and 2003 (which has since been repealed by the Data Protection Act 2018). Section 8(b) disapplied restrictions in the Data Protection Acts if processing was ‘required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders . . . in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid’. This section was, however, deeply problematic. It did not *authorise* disclosure or regulate it; it merely disapplied restrictions imposed by the Data Protection Acts. Restrictions imposed by other legislation or legal rules (such as obligations of bank secrecy or professional confidentiality) were not affected. It made it the responsibility of the data controller to determine if disclosure is necessary and proportionate – effectively outsourcing what should be a public law function.¹⁰⁵ In particular, it was insufficient to regulate access to communications data as it did not meet the criteria elaborated by the CJEU in *Digital Rights Ireland* and subsequent cases.¹⁰⁶

¹⁰⁰ See, e.g., section 110 of the Postal and Telecommunications Services Act 1983 as amended by section 30 of the Criminal Justice (Mutual Assistance) Act 2008, section 15 of the Criminal Justice Act 2011 and section 12A of the Communications (Retention of Data) Act 2011.

¹⁰¹ The reasoning in *Walsh v. National Irish Bank* [2013] IESC 2 suggests that a provider might have a defence if compliance would put it in breach of its legal obligations in another jurisdiction; however, that case concerned data held in another jurisdiction and it is not clear that the same reasoning would be applied in respect of data held in Ireland.

¹⁰² See, e.g., McIntyre, ‘Voluntary Disclosure of Data to Law Enforcement’.

¹⁰³ Murray, *Review of the Law*, 44–45; Data Protection Commissioner, ‘An Garda Síochána’, 61–62.

¹⁰⁴ ‘Law Enforcement Guidelines’, Blacknight Solutions, n.d., www.blacknight.com/legal/law-enforcement-guide-lines/.

¹⁰⁵ Data Protection Commissioner, ‘Disclosures Permitted under Section 8 of the Data Protection Act’, n.d., <https://web.archive.org/web/20130607050018/https://www.dataprotection.ie/docs/Disclosures-Permitted-under-Section-8-of-the-Data-Protection-Act-Section/237.htm>.

¹⁰⁶ See, e.g., Denis Kelleher, *Privacy and Data Protection Law in Ireland*, 2nd ed. (Haywards Heath: Bloomsbury Professional, 2015), 95.

Despite these limitations, the section came to be extensively used by providers. This was first brought to public attention by the Data Protection Commissioner audit of Facebook Ireland in 2012. That audit examined requests from law enforcement agencies to Facebook for user data, and accepted Facebook's assessment that it was entitled to disclose non-content data in response to both Irish and foreign police requests, including to law enforcement agencies outside the European Economic Area (EEA), on the basis of a case-by-case examination of each request.¹⁰⁷

This tiered approach – giving voluntary disclosure of non-content data but requiring a mutual legal assistance request or other mandatory process for content data – echoes the content/non-content distinction under US law in the Stored Communications Act.¹⁰⁸ Perhaps unsurprisingly, other major US providers appear to have carried over the same approach to their Irish operations. In a 2016 report, the Council of Europe Cybercrime Convention Committee surveyed the law enforcement guidelines of Apple, Facebook, Google, Microsoft, Twitter and Yahoo.¹⁰⁹ All bar Google and Yahoo identified Irish law as applying to at least some of the information they hold, and all of those firms drew a distinction between non-content data and content data, with the former being made available on the basis of a 'valid legal request' and the latter requiring a mutual legal assistance request or other binding legal process. That survey is now out of date, but the underlying result is significant – all the firms holding user data in Ireland appeared to take the view that they could disclose (non-content) user data without a mandatory requirement to do so under Irish law, at least in some circumstances.

12.4.3.4 Is Voluntary Disclosure Permitted after the GDPR?

The already problematic basis for voluntary disclosure has become even more dubious since the General Data Protection Regulation (GDPR) was implemented in Irish law. Section 8 of the Data Protection Acts 1988 and 2003 no longer applies, and the closest provision is section 41 of the Data Protection Act 2018, which provides:

[T]he processing of personal data and special categories of personal data for a purpose other than the purpose for which the data has been collected shall be lawful to the extent that such processing is necessary and proportionate for the purposes—

- (a) of preventing a threat to national security, defence or public security,
- (b) of preventing, detecting, investigating or prosecuting criminal offences.

The Data Protection Commission has asserted that this provides a legal basis for voluntary disclosure of data by controllers to police, though it has not given any detailed guidance on the point.¹¹⁰ But even on a preliminary assessment there are problems with this approach.

Despite a superficial resemblance, the legal effect of section 41 of the 2018 Act is quite different from that of section 8 of the Data Protection Acts 1988 and 2003. Section 41 does not completely disapply other data protection rules as the previous section did. Nor can it provide

¹⁰⁷ Data Protection Commissioner, *Facebook Ireland Report of Audit* (21 December 2011), 98–100, appendix 5, www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf; Data Protection Commissioner, *Facebook Ireland Ltd Report of Re-audit* (21 September 2012), 34–36, www.europe-v-facebook.org/ODPC_Review.pdf.

¹⁰⁸ Data Protection Commissioner, *Facebook Ireland Report of Audit*, appendix 5.

¹⁰⁹ The T-CY Cloud Evidence Group, *Criminal Justice Access to Data in the Cloud*.

¹¹⁰ Data Protection Commission, *Guidance for Drivers on Use of 'Dash Cams'* (2018, updated December 2019), www.dataprotection.ie/sites/default/files/uploads/2019-12/GuidanceforDriversontheseoffDashCams.pdf.

a free-standing legal basis for processing (given that the grounds in Articles 6 GDPR are exhaustive). Instead, section 41 merely permits processing for a purpose other than that for which the personal data was collected. This is supported by the legislative history; in a parliamentary committee, the Minister for Justice and Equality stated that section 41 was intended to provide a basis for other '[s]tatutory provisions that permit, or require, further notification of disclosure of personal data', such as obligations to report money laundering or child abuse.¹¹¹

Notwithstanding section 41 of the 2018 Act, therefore, voluntary disclosures of personal data to law enforcement still require a specific legal basis to comply with Article 6 GDPR (and Article 9 GDPR in the case of special category data). A full assessment of the power to make voluntary disclosure is beyond the scope of this chapter, but it is fair to say that it is a considerably more complex issue than the rather simplistic approach apparently endorsed by the Data Protection Commission.¹¹²

For example, in many cases of voluntary disclosure the legal basis will be the legitimate interest of the controller. In this context, a balancing test must be used which requires an individualised assessment of the need for disclosure and the impact on the data subject.¹¹³ A blanket policy of disclosing data in response to police requests will be contrary to the GDPR. Similarly, Recital 50 GDPR makes it clear that voluntary disclosure on the basis of legitimate interest cannot be relied upon if there is a countervailing obligation of secrecy in a particular case:

Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. *However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.*¹¹⁴

In practical terms, therefore, the GDPR makes an important change which should force providers with an Irish presence to reconsider voluntary disclosure practices they developed under the prior legislation; providers will be at real risk if they make voluntary disclosures without a clear legal basis for doing so, which section 41 of the Data Protection Act 2018 does not provide.¹¹⁵

¹¹¹ Charlie Flanagan TD, Oireachtas Select Committee on Justice and Equality, 3 May 2018.

¹¹² See, e.g., Thomas Kopp and Valentin Pfisterer, 'Between a Rock and a Hard Place: Legal Pitfalls of Voluntary Cooperation of German Companies with German and Foreign Regulatory and Law Enforcement Authorities' (2016) 2(2) *Compliance Elliance Journal* 24; Clare Sullivan and Eric Burger, "'In the Public Interest': The Privacy Implications of International Business-to-Business Sharing of Cyber-Threat Intelligence' (2017) 33(1) *Computer Law & Security Review* 14; Adrian Haase and Emma Peters, 'Ubiquitous Computing and Increasing Engagement of Private Companies in Governmental Surveillance' (2017) 7(2) *International Data Privacy Law* 126; Nadezhda Purtova, 'Between the GDPR and the Police Directive: Navigating through the Maze of Information Sharing in Public–Private Partnerships' (2018) 8(1) *International Data Privacy Law* 52.

¹¹³ Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC*, 844/14/EN, WP 217 (9 April 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.

¹¹⁴ Emphasis added.

¹¹⁵ Compare the judgment of the CJEU in Case C-175/20, 'SS' SIA v. *Valsts ieņēmumu dienests* [2022] ECLI:EU: C:2022:124, confirming that tax authorities require a specific legislative measure compliant with Article 5(1) GDPR to demand information from an internet advertising site regarding customers.

12.4.3.5 Is Voluntary Disclosure Permitted after the European Electronic Communications Code?

The European Electronic Communications Code (EECC)¹¹⁶ should also be mentioned as restricting the situations where voluntary disclosure might be permitted. The EECC extends the protections of the ePrivacy Directive to over-the-top communications services that qualify as ‘interpersonal communications services’, including both number-based and number-independent services. For those providers, therefore, voluntary disclosure of information about user communications is likely to constitute a breach of their obligations under the Irish transposition of the confidentiality provisions of the ePrivacy Directive.¹¹⁷

12.4.3.6 Admissibility of Data Provided through Voluntary Cooperation

Turning to admissibility, all data obtained through voluntary cooperation is capable of being used in criminal proceedings, subject to the ordinary rules of evidence. Any voluntary disclosure of information can in principle be challenged by the individual whose data is sought (for example, on the grounds that disclosure violated the data protection obligations of the provider). As with mandatory cooperation, however, the practical ability to do so will depend on whether the individual is notified, and there is no obligation in Irish law for notification. The admissibility of evidence obtained in this way can also be challenged by a defendant in any subsequent criminal trial, and the exclusionary rule will mean that such evidence may be excluded if it was obtained illegally or unconstitutionally.

12.4.4 Overview of Existing Cooperation Duties

Irish law recognises a number of means of accessing data, as already discussed throughout this chapter. The appropriate method of access in a particular investigation will depend on the type of data required, the circumstances that require the data access and whether the relevant service provider meets the definition of ‘authorised undertaking’ or ‘service provider’ in the case of interception and data retention respectively. Table 12.1 summarises the main methods and their key features.

It may also be helpful at this point to identify areas where Irish law does *not* provide for mandatory cooperation with providers. There are no provisions in Irish criminal law for real-time collection or recording of traffic or content data (other than under the interception and data retention systems), or blocking access to or takedown of web pages.¹¹⁸ Some providers may voluntarily agree to take on responsibilities – for example, some internet service providers

¹¹⁶ Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. The EECC was transposed into Irish law by the European Union (Electronic Communications Code) Regulations 2022 (SI No. 444 of 2022).

¹¹⁷ Regulation 5 of the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (SI No. 36 of 2011) as applied by Regulation 112(1)(a) of the European Union (Electronic Communications Code) Regulations 2022 (SI No. 444 of 2022).

¹¹⁸ There are some narrow exceptions. For example, in the case of internet gambling, section 32A of the Betting Act 1931, as amended by section 28 of the Betting (Amendment) Act 2015, makes it illegal to provide internet services to an unlicensed remote (online) bookmaker and authorises the Revenue Commissioners to issue an enforcement notice prohibiting such services. In relation to sanctions against Russia, the communications regulator ComReg has taken the view that Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No. 833/2014 concerning restrictive measures in view of Russia’s actions destabilising the situation in Ukraine, [2022] OJ L 65, 2 March 2022 requires Irish ISPs to block access to the Russia Today and Sputnik websites. As of January 2024, mandatory website blocking under the Terrorist Content Regulation, Regulation (EU) 2021/784 of the European

TABLE 12.1 *Summary of data access methods under Irish law*

Data access mechanism?	What type of data can be obtained?	Who can be targeted?	Legal basis and authorising body?	Grounds?
Search warrants	Any information already held by the provider (including content data); cannot require ongoing interception or generation of data. Whether passwords or decryption keys must be disclosed depends on the type of crime and the precise statutory power relied upon.	A search warrant can be issued in respect of any place in the state, including locations of telecoms providers; information society service providers generally; and over-the-top services.	Various statutory powers depending on the offence being investigated, e.g. section 7 of the Criminal Justice (Offences Relating to Information Systems) Act 2017 for most cyber-crime offences. Court ordered.	Generally limited to investigation etc. of offences carrying a possible five-year prison sentence.
Production orders	Any information already held by the provider (including content data); cannot require ongoing interception or generation of data. Whether passwords or decryption keys must be disclosed depends on the type of crime and the precise statutory power relied upon.	Any natural or legal person in the state/ carrying on business in the state can be issued with a production order, including: telecoms and connectivity providers; information society service providers generally; and over-the-top services.	Various statutory powers depending on the offence being investigated, e.g. section 15 of the Criminal Justice Act 2011. Court ordered.	Generally limited to investigation etc. of offences carrying a possible five-year prison sentence.
Interception warrants	Telecommunications messages (content); warrants may require interception on an ongoing basis or access to stored telecommunications messages.	Only ‘authorised undertakings’: essentially traditional telecoms and connectivity providers but not, e.g., over-the-top communication services, webmail providers or other information society services.	Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993. Requires a warrant signed by the Minister for Justice and Equality.	Investigation etc. of serious offences (defined as carrying a possible five-year prison sentence and meeting additional criteria such as loss of life, serious personal injury, substantial gain or other especially serious factors); security of the state.

TABLE 12.1 (*continued*)

Data access mechanism?	What type of data can be obtained?	Who can be targeted?	Legal basis and authorising body?	Grounds?
Access to retained data	User data, internet source data, Schedule 2 data (location and communications traffic data).	Applies only to 'service providers': essentially traditional telecoms and connectivity providers but not, e.g., over-the-top communication services, webmail providers or other information society services.	Communications (Retention of Data) Act 2011. Requires internal authorisation within police and other investigative agencies (user data) or judicial authorisation (internet source data and Schedule 2 data). There are exceptions to the requirement of judicial authorisation in cases of urgency.	Varies according to the data sought. User data is available in relation to investigation etc. of criminal offences generally, as well as revenue offences; police disciplinary matters; the security of the state; the saving of human life; and locating a missing person. Internet source data is available in relation to investigation etc. of serious offences (carrying a possible five-year prison sentence); revenue offences; police disciplinary matters; the security of the state; the saving of human life; and locating a missing person. Schedule 2 data is generally available only in relation to state security, unless the data is being held for a purpose other than compliance with a High Court order imposing data retention obligations, in which case it is also available in relation to serious offences, revenue offences and police disciplinary matters.

TABLE 12.1 (*continued*)

Data access mechanism?	What type of data can be obtained?	Who can be targeted?	Legal basis and authorising body?	Grounds?
Voluntary access to user data	Potentially any information, but, in practice, usually non-content data only.	Any data controller based in Ireland. This can include telecoms providers, information society service providers and over-the-top communication services.	Section 41 of the Data Protection Act 2018. (Previously section 8 of the Data Protection Acts 1988 and 2003.) No official authorisation is required by law; in practice, providers usually require sign-off by a senior official in the relevant agency.	Investigation etc. of offences, national security, defence and public security.

(ISPs) voluntarily block access to websites said to contain child abuse images¹¹⁹ – but there is no legal framework around these areas. There is no provision in Irish law for data preservation (quick freeze) orders in support of criminal investigations, except in relation to those traditional telecommunications and connectivity providers such as mobile phone operators who are ‘service providers’ within the scope of the Communications (Retention of Data) Act 2011.¹²⁰

12.4.4.1 Encryption

As discussed in Section 12.2.1, whether a statutory power requires disclosure of encryption keys or decrypted text depends on the exact power used. Production orders usually require information to be produced in a form in which it is ‘visible and legible’.¹²¹ For example, section 15(6) of the Criminal Justice Act 2011 provides that:

Where the documents concerned are not in legible form, an order under this section shall have effect as an order—

- (a) to give to a member of the Garda Síochána any password necessary to make the documents legible and comprehensible,
- (b) otherwise to enable the member of the Garda Síochána to examine the documents in a form in which they are legible and comprehensible, or
- (c) to produce the documents to the member of the Garda Síochána in a form in which they can be removed and in which they are, or can be made, legible and comprehensible.

Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance), [2021] OJ L 172, 17 May 2021, has not been implemented in Irish law.

¹¹⁹ T. J. McIntyre, ‘Cybercrime in Ireland: Towards a Research Agenda’, in Deirdre Healy, Claire Hamilton, Yvonne Daly and Michelle Butler (eds.), *The Routledge Handbook of Irish Criminology* (Abingdon: Routledge, 2015), 110–111.

¹²⁰ Communications (Retention of Data) Act 2011, ss. 7A and 7B.

¹²¹ See, e.g., Criminal Justice (Theft and Fraud Offences) Act 2001, s. 52.

This means that, for example, a provider ordered to disclose data which it holds on behalf of a user will have to remove any encryption applied by the provider itself. However, it will not require decryption of data where the key is held by the user, or backdooring of systems such as end-to-end encryption.¹²²

Some search warrants give police the power to require a person with access to a computer at the location being searched to provide relevant passwords and encryption keys that are necessary to render information visible and legible.¹²³ But note that these powers relate to individuals who are physically present at a particular place while it is being searched – they are not free-standing powers to demand passwords or encryption keys in other circumstances. There are no specific provisions to safeguard rights in the context of encrypted information, and decrypted data is admissible in criminal proceedings subject to the ordinary rules of evidence.

12.4.4.2 Law Enforcement Agency Hacking

Irish law does not specifically provide for state hacking.¹²⁴ It is possible that state malware could be used as a ‘surveillance device’ under the regime established by the Criminal Justice (Surveillance) Act 2009; however, there is no public information as to whether this has happened or whether Irish police have this capability.¹²⁵ It should be noted that the 2009 Act does not permit the use of surveillance devices in a way that would amount to an ‘interception of communications’ as defined by the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, so that if state malware is deployed it would have to be tailored to avoid capturing phone calls, text messages and emails if they fall within the scope of the 1993 Act.¹²⁶

12.4.4.3 Interception Capability Requirements

There is no general statutory power requiring providers to change the technical infrastructure or security settings of their services to make them vulnerable to interception. However, in relation to ‘authorised undertakings’ (traditional telecommunication providers), a government Minister may issue directions in writing, requiring them to do anything which the Minister may specify from time to time as necessary in the national interest.¹²⁷ These directions are kept secret, but appear to include requirements to build in intercept capability.¹²⁸

¹²² Given the principle that powers infringing on privacy must be strictly construed, and the practical and financial impact of requiring a provider to attempt to undermine user encryption or backdoor their system, this section must be read as only requiring disclosure of a password held by a provider rather than any more invasive actions. See, e.g., *Byrne v. Grey* [1988] IR 31.

¹²³ See, e.g., Criminal Justice (Offences Relating to Information Systems) Act 2017, s. 7(4).

¹²⁴ Without some statutory basis, state malware would most likely constitute the offence of accessing an information system without lawful authority contrary to section 2 of the Criminal Justice (Offences Relating to Information Systems) Act 2017.

¹²⁵ The Irish authorities have stated that ‘[s]urveillance warrants can be obtained under the Criminal Justice (Surveillance) Act 2009 to monitor computers that use encryption, and this can overcome difficulties in serious criminal cases where it is known that encryption is being used and passwords will not be handed over’. It is not clear whether this refers to hacking, but the context suggests that it does. See, e.g., Council of the European Union, *Report on Ireland*, 68.

¹²⁶ Criminal Justice (Surveillance) Act 2009, s. 2(3).

¹²⁷ Section 110 of the Postal and Telecommunications Services Act 1983 (as amended). There is an obvious question mark as to whether such a wide power, exercised in secret, is a sufficient legal basis for the purposes of Article 8 ECHR.

¹²⁸ In 2016 a ministerial answer to a parliamentary question stated: ‘Telecommunications services providers are required to maintain a capacity to intercept telecommunications messages in accordance with the provisions of section 110 of

12.4.4.4 Territorial Scope

The number of providers with a presence in Ireland but operations elsewhere means that the territorial scope of domestic powers is of crucial importance. In addition to determining which providers come within the scope of these powers, we must also determine whether it is possible to compel those providers to disclose data hosted outside the state. To put it another way: does Irish law permit any extraterritorial jurisdiction similar to that asserted by the United States in the *Microsoft Ireland* litigation? The answer will depend in each case on the nature of the power being used.

12.4.4.5 Search Warrants

Search warrants are inherently territorial and so can only be granted in respect of premises located within the state (the location of the individual whose data is sought is irrelevant). Some search warrants, however, appear to permit access to data held on computers outside the state where it is accessible by means of a computer at the place being searched. Consider, for example, section 7 of the Criminal Justice (Offences Relating to Information Systems) Act 2017. Search warrants under this section permit a member of An Garda Síochána to ‘operate any computer at the place that is being searched’.¹²⁹ However, the section defines ‘computer at the place that is being searched’ to include ‘any other computer, *whether at the place being searched or at any other place*, which is lawfully accessible by means of that computer’.¹³⁰ On the face of it, this permits ‘remote searches’ or ‘network searches’, including searches of computers located in other jurisdictions. It would, for example, seem to permit access to webmail hosted abroad where a device at the place being searched is logged in to that service. This presents difficult comity issues, particularly where such searches would not be permitted in those other jurisdictions, and it is surprising that the legislative history for this section does not address this point.¹³¹

12.4.4.6 Production Orders

A similar point arises in respect of production orders, which are territorial in the sense that they are available against any person in the state¹³² who has ‘possession or control’ of documents but do not necessarily require that the *documents* must also be located within the state.¹³³ For example, under section 15(18) of the Criminal Justice Act 2011, a District Court judge has jurisdiction to make a production order if a company carries on business in the relevant district, whether or not the documents are also located in that district.¹³⁴

the Postal and Telecommunications Services Act 1983, as amended. The State does not reimburse the costs associated with this.’ Frances Fitzgerald, Written Answers, Dáil Éireann, 16 September 2016, 171.

¹²⁹ Criminal Justice (Offences Relating to Information Systems) Act 2017, s. 7(4)(a).

¹³⁰ Criminal Justice Act 2017, s. 7(9). Emphasis added.

¹³¹ For background on remote searches. See, e.g., Susan Brenner, ‘Law, Dissonance, and Remote Computer Searches’ (2012) 14(1) *North Carolina Journal of Law & Technology* 43; Bert-Jaap Koops and Morag Goodwin, *Cyberspace, the Cloud, and Cross-Border Criminal Investigation: The Limits and Possibilities of International Law* (Tilburg: TILT, 2014), https://repository.wodc.nl/bitstream/handle/20.500.12832/2047/2326-volledige-tekst_tcm28-73009.pdf?sequence=2&isAllowed=y.

¹³² These powers generally apply to a person ‘carrying on business in the state’ also. There is no case law as to whether ‘carrying on business in the state’ would include providers who serve Irish customers but who do not have any physical presence in the state.

¹³³ The location of the individual whose data is being sought is also irrelevant.

¹³⁴ Criminal Justice Act 2011, s. 15(18), emphasis added. Section 52 of the Criminal Justice (Theft and Fraud Offences) Act 2001 creates a similar power with the same uncertainty as to its scope.

The better argument is probably that these production order powers are implicitly limited to documents within the state¹³⁵ – under section 15(5) of the Criminal Justice Act 2011, for example, it is possible to grant an order for entry to the place where documents are kept, which would be inappropriate in relation to documents held in another state – but this and similar statutory powers are not clear on this point. There is no case law directly on this issue, but in *Walsh v. National Irish Bank*¹³⁶ the Supreme Court held that an equivalent revenue law power could be used to order disclosure of documents held by a foreign branch of an Irish bank, unless to do so would put the bank in breach of foreign law.

It may be that discussion of the extraterritorial scope of search warrants and production orders is moot. In the 2017 European Council Mutual Evaluation on Combating Cybercrime, the Irish authorities summarised their understanding of Irish law as being that providers can only be obliged to produce evidence ‘located in Ireland’.¹³⁷ It seems unlikely that they will subsequently take a different interpretation – given the importance of the internet industry in Ireland there would be political costs in doing so, and by opting in to the e-Evidence proposals, Ireland will in any event benefit from extraterritorial jurisdiction. Nevertheless, the lack of certainty on this point is undesirable.

12.4.4.7 Interception of Communications and Data Retention

The interception and data retention powers apply to ‘authorised undertakings’ and ‘service providers’.¹³⁸ As already discussed, these terms are defined in accordance with the EU telecommunications framework.¹³⁹ The legislation does not address the question of territorial scope, but in principle any such provider who is providing a service in Ireland would appear to be within the scope of these powers, regardless of the location of the headquarters or data storage. The legislation does not make these powers contingent on the location of the individual, and in principle these powers can be exercised in respect of an individual located abroad. Where an interception of communications is carried out in relation to an individual elsewhere in the EU then the other member state must be notified in accordance with the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.¹⁴⁰ There is no similar requirement in relation to access to retained data.

12.4.5 Legal Remedies and Protection of Fundamental Rights

Irish law has long failed to provide adequate fundamental rights safeguards around state surveillance; instead, the state has adopted a reactive approach where reform has been a grudging and minimal response to scandal and litigation.¹⁴¹ A full account of the fundamental rights issues around access to data processed by providers is beyond the scope of this chapter, but a number of aspects should be highlighted.

¹³⁵ Compare *Chemical Bank v. McCormack* [1983] ILRM 350 and *Walsh v. National Irish Bank* [2007] IEHC 325, discussed in Law Reform Commission, *Report on Search Warrants and Bench Warrants*.

¹³⁶ *Walsh v. National Irish Bank* [2013] IESC 2.

¹³⁷ Council of the European Union, *Report on Ireland*, 109.

¹³⁸ Communications (Retention of Data) Act 2011; Regulations 2003 (SI 306 of 2003).

¹³⁹ Regulations 2003 (SI 306 of 2003), regulation 4.

¹⁴⁰ Criminal Justice (Mutual Assistance) Act 2008, s. 26.

¹⁴¹ T. J. McIntyre, ‘Implementing Information Privacy Rights in Ireland’, in Suzanne Egan (ed.), *Implementing Human Rights in Ireland* (Dublin: Bloomsbury Academic, 2015), 271–287; Maria Helen Murphy, ‘The Relationship between the European Court of Human Rights and National Legislative Bodies: Considering the Merits and the Risks of the Approach of the Court in Surveillance Cases’ (2013) 3(2) *Irish Journal of Legal Studies* 65; Maria Helen Murphy, ‘Surveillance and the Right to Privacy: Is an “Effective Remedy” Possible?’, in Alice Diver and Jacinta Miller (eds.), *Justiciability of Human Rights Law in Domestic Jurisdictions* (Heidelberg: Springer, 2015), 289–306.

12.4.5.1 Notification

There is no provision in Irish law requiring that individuals be notified of the fact that their data has been accessed (except where Schedule 2 data is accessed under the Communications (Retention of Data) Act 2011). This is the case regardless of whether the individual is a suspect or notification would present a risk to an ongoing investigation. As already mentioned, some of the major US providers such as Apple, Facebook, Microsoft and Yahoo do commit to notifying users where their personal information is sought (subject to limitations), but this is purely a matter of policy on their part.¹⁴²

12.4.5.2 Redress

In relation to interception and data retention, there is a statutory complaints mechanism that permits an individual to apply to a ‘Complaints Referee’ (usually a sitting Circuit Court judge) to investigate whether a ministerial authorisation for interception or a disclosure requirement for data was made and, if so, whether the requirements of the relevant act were followed in respect of the request.¹⁴³ This is an inquisitorial procedure: the Referee has the power to access any official documents relating to the measure. If the Referee concludes that the law has been contravened, they must notify the applicant in writing of that conclusion and make a report of their findings to the Taoiseach (Prime Minister). The Referee may also, if they think fit, quash the ministerial authorisation, direct the relevant agency to destroy the information obtained and recommend the payment of compensation to the complainant.

This redress system is, however, very limited. It is essentially limited to investigating whether a ministerial warrant or disclosure requirement was issued properly – it does not provide a remedy in relation to other situations such as improper retention or disclosure by the telecommunications provider, or misuse of data by police. The remedies are discretionary rather than a matter of right – in each case the destruction of the information obtained and the award of compensation are only if the Complaints Referee ‘thinks fit’. There is almost no transparency regarding the activities of the Complaints Referee; investigations and decisions are not publicised and the Irish government has stated that it does not hold records on the number of complaints received or any details of such complaints.¹⁴⁴ However, it seems that there has never been a successful complaint to the Complaints Referee.¹⁴⁵

12.4.5.3 Oversight

In relation to interception of communications and data retention, there is judicial oversight by a ‘designated judge’ (a sitting judge of the High Court) who has the duty of keeping the operation of the legislation under review and publishing annual reports.¹⁴⁶ In practice, this consists of yearly meetings with officials from the Department of Justice, the police and other agencies who use interception and data retention powers, and some inspection of their files.

¹⁴² The T-CY Cloud Evidence Group, *Criminal Justice Access to Data in the Cloud*, s. 2.2.5.

¹⁴³ Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, s. 9; Communications (Retention of Data) Act 2011, s. 10.

¹⁴⁴ Dan MacGuill, ‘State Surveillance: How Gardaí and Others Can Secretly Monitor You’, *Journal*, 17 May 2015, www.thejournal.ie/state-surveillance-ireland-gardai-wiretapping-email-monitoring-gardai-2099537-May2015/.

¹⁴⁵ See, e.g., the answer of the Minister for Justice, Equality and Law Reform to a parliamentary question on this point. Brian Lenihan, Written Answers, Dáil Éireann, 4 March 2008, 11, 148, 501 and 502.

¹⁴⁶ Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993, s. 8; Communications (Retention of Data) Act 2011, s. 11.

However, the effectiveness of this process, like the Complaints Referee procedure, has been strongly criticised.¹⁴⁷ The oversight role is a part-time function of a judge with a full judicial caseload. The role has no staff and no specialist legal or technical support, meaning that there is no institutional memory and making it dependent on the entities being monitored. Until quite recently the annual reports almost always consisted of one or two pages with a few formulaic paragraphs reciting that, on a particular day, certain (unspecified) documents were inspected, certain (unspecified) queries were answered and, as a result, the judge was satisfied that the relevant authorities were in compliance with the law.¹⁴⁸

One recently appointed designated judge took some steps to address these criticisms. In her 2018 annual report, Baker J. provides slightly more detail on the operation of these systems.¹⁴⁹ However, that report still came to a total of only four pages and illustrates weaknesses in the oversight system. Although Baker J. identified the data retention system as contrary to European fundamental rights standards following *Tele2*, she lacked the power to require that it be suspended until a proper legal basis was established and no action was taken on the basis of her report.

12.4.5.4 Failings in the Current Legal Framework

It is clear that significant reform of Irish law on access to data is required to achieve even bare compliance with ECHR and Charter of Fundamental Rights requirements.¹⁵⁰ A full account of these European norms and the deficiencies of the existing legal framework is beyond the scope of this chapter, but, drawing on the discussion earlier in the chapter, we can briefly summarise the main areas where reform is needed.

The Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 fails to provide sufficient safeguards for data subjects. Notably absent from the regime are a requirement for judicial authorisation, procedures for notification where notification would not be prejudicial to an investigation, an effective oversight process and transparent procedures allowing for adequate redress. In addition, the 1993 Act permits interception of journalists' communications without prior judicial authorisation, contrary to the standards established by the ECtHR in *Telegraaf Media v. the Netherlands*,¹⁵¹ and similarly fails to protect lawyer–client privileged communications.

The Communications (Retention of Data) Act 2011 still fails to address the majority of the issues identified in the Murray report, notwithstanding the changes made by the Communications (Retention of Data) (Amendment) Act 2022. The definition of 'serious offence' is excessively broad and permits disproportionate access to personal data. There is no definition of the national security purposes that justify access to data. As with interception, there are no

¹⁴⁷ T. J. McIntyre, 'Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective', in Martin Scheinin, Helle Krunke and Marina Aksenova (eds.), *Judges as Guardians of Constitutionalism and Human Rights* (Cheltenham: Edward Elgar, 2016).

¹⁴⁸ The annual reports of the designated judge and other official materials are available at Digital Rights Ireland, 'Surveillance Library', <https://web.archive.org/web/20220120104440/https://www.digitalrights.ie/irish-surveillance-documents/>.

¹⁴⁹ Marie Baker, *Report of Designated Judge Made Pursuant to Section 8(2) of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 and Section 12(1)(c) of the Communications (Retention of Data) Act 2011* (Houses of the Oireachtas, 28 June 2018), http://opac.oireachtas.ie/AWDData/Library3/TAOdoclaido2o82o18d_113723.pdf.

¹⁵⁰ McIntyre, 'Judicial Oversight of Surveillance'; Murphy, 'Surveillance and the Right to Privacy'.

¹⁵¹ *Telegraaf Media v. The Netherlands*, Appl. No. 39315/06, 22 November 2012.

protections in place in relation to journalists' sources. The 2011 Act also fails to provide a cause of action for wrongful access to data.

The reliance by Irish police on voluntary disclosure by providers is also problematic. The intrusiveness of this practice is mitigated somewhat by the fact that the most important providers provide only non-content data in this way, but it is astonishing that stored over-the-top communications, subscriber information and communications metadata can be provided without any clear legal basis, prior judicial approval, notification, subsequent judicial oversight or redress mechanism. In permitting access to the *content* of communications in this way, Ireland fails to meet the requirements of ECHR case law from *Klass v. Germany* onwards, which requires that at a minimum there must be oversight mechanisms established by law that are 'independent of the authorities carrying out the surveillance', 'objective' and 'vested with sufficient powers and competence to exercise an effective and continuous control' over communications surveillance.¹⁵²

Even in relation to *non-content data*, this voluntary disclosure is of very dubious legality. In relation to subscriber data, for example, there is considerable authority that identifies the sensitivity of this data as requiring a statutory basis for disclosure. In *R v. Spencer*,¹⁵³ the Canadian Supreme Court held that a police request for voluntary disclosure of subscriber information from an ISP was a search that violated section 8 of the Canadian Charter of Rights. This was notwithstanding a provision in the Personal Information Protection and Electronic Documents Act (PIPEDA) which permitted disclosure where a law enforcement agency had requested personal information and had 'lawful authority' to do so; the Supreme Court took the view that 'lawful authority' in this context meant a compulsory power to require disclosure, not merely a power to ask. The 2018 ECtHR judgment in *Benedik v. Slovenia*¹⁵⁴ reaches a very similar result in holding that Slovenia violated Article 8 ECHR by failing to provide an adequate legal framework around access to ISP subscriber information. In light of these precedents, Irish practice is on shaky ground.

In addition to changes to the rules regarding access to data, it will be important to introduce an effective institutional framework to ensure that those rules are followed. The EU Fundamental Rights Agency has recommended in relation to state surveillance that

[t]he independence of oversight bodies should be enshrined in law and applied in practice. EU Member States should grant oversight bodies adequate financial and human resources, including diverse and technically-qualified professionals. Member States should also grant oversight bodies the power to initiate their own investigations as well as permanent, complete and direct access to necessary information and documents for fulfilling their mandate. Member States should ensure that the oversight bodies' decisions are binding.¹⁵⁵

In line with this recommendation, the designated judge role should be replaced by an oversight body, chaired by a judge with support from legal and technical specialists, with binding powers to order the cessation of surveillance activities. At the time of writing (February 2024) there is some reform taking place: the role of the designated judge is in the process of being transferred to a newly established Independent Examiner of Security Legislation under the Policing, Security

¹⁵² *Klass v. Germany*, Appl. No. 5029/71, 6 September 1978, para. 56.

¹⁵³ *R. v. Spencer*, 2014 SCC 43, [2014] 2 SCR 212.

¹⁵⁴ *Benedik v. Slovenia*, Appl. No. 62357/14, 24 April 2018.

¹⁵⁵ European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU – Field Perspectives and Legal Update*, 2 vols. (Luxembourg: Publications Office of the European Union, 2017), vol. II, p. 11, <https://publications.europa.eu/en/publication-detail/-/publication/b7f98a74-afc2-11e7-837e-01aa75cd71a1/language-en>.

and Community Safety Act 2024. This, however, is largely a change of personnel rather than function – the new Independent Examiner will have the same limited role and powers as the designated judge – and is not enough to ensure adequate oversight.

12.5 CROSS-BORDER COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

12.5.1 *Introduction*

Despite the growing importance of Ireland as a centre for internet firms, there is little domestic law on the issue of cross-border cooperation in relation to access to data held by providers. The following subsections outline the current state of play on important matters, including the potential ratification of the Cybercrime Convention.

12.5.1.1 Convention on Cybercrime

Ireland signed the Cybercrime Convention on 28 February 2002 but has yet to ratify it.¹⁵⁶ Until 2017, domestic law failed to address either the substantive offences or the procedural provisions required by the Convention. In 2017, the substantive offences were finally transposed into Irish law, but there is still no legislation in place dealing with the procedural provisions, such as expedited preservation of data.¹⁵⁷

12.5.1.2 European Investigation Order

Ireland chose not to opt into the draft EIO Directive when it was proposed in 2010. In 2014, the then Minister for Justice and Equality, Frances Fitzgerald, explained that this was on the basis that the draft directive was ‘inconsistent with Irish law and practice’, in particular owing to the limited grounds for non-recognition and non-execution of an EIO and the lack of a general dual criminality requirement.¹⁵⁸ The Minister indicated that Ireland would consider opting in to the EIO, but as of December 2022 this has not happened.

12.5.1.3 MLA Agreements and Criminal Justice (Mutual Assistance) Act 2008

In the absence of powers under the Cybercrime Convention or the EIO Directive, the primary legal basis for cross-border cooperation are the mutual legal assistance (MLA) agreements to which Ireland is a party. These are given legal effect by the Criminal Justice (Mutual Assistance) Act 2008, which designates the Minister for Justice and Equality as the Central Authority for the purposes of dealing with requests.¹⁵⁹

Ireland does not publish statistics on the number of MLA requests made to or by the Irish authorities. However, a 2017 evaluation of Irish practice regarding cybercrime provides

¹⁵⁶ For background, see, e.g., McIntyre, ‘Cybercrime in Ireland’.

¹⁵⁷ The offences were transposed by the Criminal Justice Act 2017. There is limited provision for preservation of some communications data under the Communications (Retention of Data) Act 2011.

¹⁵⁸ Frances Fitzgerald, Written Answers, Dáil Éireann, 4 June 2014, 164–166.

¹⁵⁹ See, e.g., Department of Justice and Equality, *Mutual Legal Assistance in Criminal Matters: A Guide to Irish Law and Procedures* (July 2008).

a snapshot: in 2015 the central authority received 615 incoming MLA requests (of which approximately 160 were for material stored by providers in Ireland) and 250 outgoing requests.¹⁶⁰ Seventy-seven of these outgoing requests were to the United States, and these were described as ‘primarily’ for material stored by providers.¹⁶¹ It should be noted that these figures significantly understate the extent to which there is international cooperation in this area – because they are limited to cases where the MLA procedure is used, they will not capture situations where firms with an Irish presence respond to overseas requests on a voluntary basis. Similarly, these statistics may not fully reflect the extent to which Irish authorities rely on material from the large providers; for example, requests to Facebook (for non-content data) may have been made under domestic law to Facebook Ireland Ltd rather than through the MLA process.¹⁶²

12.5.1.4 Data Localisation

Irish law does not have any distinct data localisation rules for providers. The only applicable rules are the ordinary rules of EU data protection law prohibiting transfer to third countries.

12.5.2 *Cooperation of National LEAs with Foreign Service Providers (Outbound Requests from Ireland): Legal Framework and Nature of the Cooperation*

12.5.2.1 Access to Data

The Criminal Justice (Mutual Assistance) Act 2008 provides the legal framework for access by Irish police to data held by foreign providers. In general, it applies to ‘designated states’ – defined as EU member states and other states designated by the Minister for Foreign Affairs.¹⁶³

The most important provisions are sections 62 and 73, which provide for taking evidence from a person in a designated state and searching for evidence at a place in a designated state. In any criminal investigations or criminal proceedings, the Director of Public Prosecutions or a judge may send a letter of request to the Central Authority specifying the evidence which is sought and including:

- a statement that the evidence is required for the purpose of criminal proceedings or a criminal investigation,
- a brief description of the conduct constituting the offence concerned and
- any other available information that may assist the appropriate authority in complying with the request.

When evidence is obtained under these sections, its use is restricted. The evidence may not be used for any purpose other than that permitted by the relevant international instrument or specified in the letter of request without the consent of the appropriate authority in the designated state. When the evidence is no longer required for that purpose (or for any other purpose for which such consent has been obtained), it must be returned to the appropriate

¹⁶⁰ Council of the European Union, *Report on Ireland*, 103.

¹⁶¹ Ibid.

¹⁶² See, e.g., Data Protection Commissioner, *Facebook Ireland Report of Audit*, 99.

¹⁶³ Criminal Justice (Mutual Assistance) Act 2008, s. 4.

authority unless the authority indicates that it need not be returned. Both sections 62 and 73 also provide for this evidence to be admissible without further proof.

12.5.2.2 Interception of communications

Requests for interception of communications are regulated by part 3 of the Criminal Justice (Mutual Assistance) Act 2008, which gives effect to Articles 17 to 22 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union 2000. Section 23 deals with the situation where technical assistance is needed from a member state,¹⁶⁴ and provides that the Minister for Justice may request a competent authority in another member state to carry out interception for transmission to the Garda Síochána. Section 26 addresses the situation where a telecommunications address is being used in another member state and technical assistance is not required for an interception to be carried out, and provides for notification by the Minister of the competent authority in the relevant state.

In each case, however, these provisions apply only where the Minister has given an authorisation for an interception under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993. As already discussed, that legislation applies only to messages being transmitted by ‘authorised undertakings’ and therefore does not apply to over-the-top communication services, which fall outside the scope of the telecommunications law framework.¹⁶⁵

The result is a significant gap in that the Criminal Justice (Mutual Assistance) Act 2008 does not permit the Minister to seek interception of communications on over-the-top services in other member states – even where the domestic law of those member states does provide for such interception.¹⁶⁶

12.5.2.3 Legal Remedies and Protection of Human Rights

Section 107 of the Criminal Justice (Mutual Assistance) Act 2008 enforces any restrictions in MLA treaties on the use of personal data obtained from another jurisdiction by providing that the ‘provisions of the relevant international instrument have effect in respect of the use of personal data communicated to or otherwise obtained by a person in the State under the instrument’. It also confirms that data protection law applies in respect of the data. The 2008 Act otherwise does not create any additional legal remedies or specific fundamental rights safeguards regarding to access to data held outside Ireland or interception of communications outside Ireland.

12.5.2.4 Irish Views on the Effectiveness of the MLA Process

In the 2017 European Council Mutual Evaluation on Combating Cybercrime, the Irish authorities ‘stressed the fact that the MLA process is time-consuming and the processes can be cumbersome’.¹⁶⁷ This reflects a general view within Irish police; for example, one garda (police

¹⁶⁴ Defined in section 2 of the Criminal Justice (Mutual Assistance) Act 2008 to mean other EU member states, plus Iceland and Norway and any other state which might be designated under section 4. No other states have been yet designated for the purpose of part 3 of the Act on interception of communications.

¹⁶⁵ Denis Kelleher, *Privacy and Data Protection Law in Ireland* (Dublin: Tottel, 2006), 454.

¹⁶⁶ Access to stored communications would still be possible through a request under section 62 or section 73 of the Criminal Justice (Mutual Assistance) Act 2008; however, requests for real-time interception would be precluded.

¹⁶⁷ Council of the European Union, *Report on Ireland*, 109.

officer) was quoted anonymously in the media as saying that social media investigations are significantly hampered by the delay in receiving responses to MLA requests.¹⁶⁸

12.5.3 *Cooperation of National Service Providers with Foreign LEAs (Inbound Requests to Ireland)*

12.5.3.1 Mandatory Cooperation

The Criminal Justice (Mutual Assistance) Act 2008 requires Irish providers to provide information to foreign law enforcement agencies in response to an MLA request. The key provisions are sections 24 and 25, dealing with incoming requests for interception of telecommunications messages, and sections 63, 74 and 75 on the taking of evidence and searches for evidence.

12.5.3.2 Taking Evidence: Questioning Witnesses

Section 63 of the Criminal Justice (Mutual Assistance) Act 2008 deals with inbound requests for evidence to be taken from a witness, for the purpose of criminal proceedings or a criminal investigation in a designated state. Taking evidence in this context primarily means questioning witnesses, but may also involve a witness being compelled to produce a document.

On receiving such a request, the Minister for Justice and Equality may¹⁶⁹ request the President of the District Court to nominate a judge to receive the evidence; doing this confers on that judge the powers of the District Court in criminal proceedings, including the power to compel witnesses and to secure the production of documents.¹⁷⁰ Failure to give evidence or to produce a document, without reasonable excuse, is an offence carrying a possible fine of €2,500 or imprisonment for up to six months. There is no requirement of dual criminality in relation to this power. Witnesses may assert any applicable privilege which would apply in criminal proceedings either in Ireland or in the state seeking the evidence.¹⁷¹

12.5.3.3 Access to Data

Sections 74 and 75 of the Criminal Justice (Mutual Assistance) Act 2008 deal with inbound requests for searches for evidence for use outside Ireland. Of these, section 75 is most relevant for the majority of cases involving access to data.

¹⁶⁸ Cathal McMahon, 'Gardaí Dealing with Avalanche of Social Media Complaints Claim "Unnecessary Obstacles" Put in the Way by Management and Web Firms', *Independent*, 29 April 2017, www.independent.ie/irish-news/news/garda-dealing-with-avalanche-of-social-media-complaints-claim-unnecessary-obstacles-put-in-the-way-by-management-and-web-firms-35664310.html.

¹⁶⁹ The power is a discretionary one. In *Agrama v. Minister for Justice, Equality and Law Reform* [2015] IESC 94, O'Donnell J. noted, regarding the precursor provision to section 63 of the 2008 Act:

Having regard to the objective of mutual assistance, it will be only on rare occasions that the Minister would refuse. Refusal would normally require compelling reasons. It is not possible or desirable to provide an exhaustive list of the circumstances which would justify refusal. Such circumstances must be considered by reference to the facts of the individual case, but grounds which might amount to compelling reasons justifying refusal may be considerations such as national security, breach of a fundamental principle of justice, or abuse of the process. (para. 35)

Note that under section 3 of the Criminal Justice (Mutual Assistance) Act 2008 certain threats to fundamental rights will *require* that assistance be refused.

¹⁷⁰ Criminal Justice (Mutual Assistance) Act 2008, s. 63(4).

¹⁷¹ *Ibid.*, s. 64.

The criteria for section 75 to apply are as follows:

- There must be a request from a designated state or a member state for evidential material.¹⁷²
- The request must be for the purpose of criminal proceedings or a criminal investigation.¹⁷³
- The alleged conduct would create a power under Irish law to issue a search warrant.¹⁷⁴
- In the case of a request from a member state:
 - the conduct must be punishable by both Irish law and the law of the requesting state by 6 months' imprisonment; or
 - the conduct must be punishable by Irish law by 6 months' imprisonment and must be an infringement of the rules of law of the requesting state, being prosecuted by the administrative authorities, where the decision may give rise to proceedings before a court having jurisdiction in criminal matters;¹⁷⁵
- In the case of a request from a designated state (other than a member state) the conduct in question must meet the standard of dual criminality.¹⁷⁶

Where these criteria apply, the Minister for Justice and Equality may send the request to the Commissioner of the Garda Síochána to be complied with. If the Garda Síochána already has possession of the relevant material (for example, if a parallel domestic investigation is underway), it may be supplied in response to the request; otherwise, a member of the Garda of at least inspector rank shall apply to a District Court judge for an order in relation to the material¹⁷⁷ and that order may be granted if the judge is satisfied that there are reasonable grounds for believing that the person named in the order possesses the evidential material.¹⁷⁸

The order which may be granted under section 75(10) of the Criminal Justice (Mutual Assistance) Act 2008 is effectively a hybrid production order and search warrant, requiring production of the specified evidential material or giving access to it, and granting a member of the Garda Síochána power to enter and search the relevant place for the material, if necessary. It is a crime to obstruct a member of the Garda Síochána acting under an order, or to fail to comply with a requirement in the order.¹⁷⁹

There is limited provision for decryption under section 75(11), which requires data to be provided in plaintext but will not require decryption of data where the key is held by the user, or backdooring of systems such as end-to-end encryption.¹⁸⁰ It should also be noted that, unlike some other statutory powers, this provision does not give police power to demand disclosure of a password or encryption key for the requested data; they are empowered to demand disclosure of merely the data itself in decrypted form.¹⁸¹

12.5.3.4 Interception of Communications

Inbound requests to the Irish authorities for interception of communications are regulated by sections 24 and 25 of the Criminal Justice (Mutual Assistance) Act 2008. Section 24 provides that

¹⁷² Ibid., s. 75(1).

¹⁷³ Ibid.

¹⁷⁴ Ibid.

¹⁷⁵ Ibid., s. 74(2).

¹⁷⁶ Ibid., s. 75(3).

¹⁷⁷ Ibid., s. 75(8).

¹⁷⁸ Ibid., s. 5(9).

¹⁷⁹ Ibid., s. 75(16).

¹⁸⁰ See the discussion of similar statutory wording in Section 12.4.4 of this chapter.

¹⁸¹ Unless the password or encryption key is itself the requested evidence.

member states may request the Irish state to carry out interceptions for the purpose of criminal investigations if a lawful interception order has been issued in that member state. This covers two situations: where the person against whom the order applies is in Ireland, and where the person is in another member state but technical assistance from the Irish state is needed to intercept the messages. Requests are to be made by a competent authority in the requesting member state to the Minister for Justice.

Section 25 then sets out the basis on which the Minister may authorise the interception. To summarise:

- Where the person is outside Ireland, the Minister may authorise the interception if the requirements of section 24 are met (with no requirement of dual criminality or that the conduct would be a serious offence under Irish law).¹⁸²
- Where the person is in Ireland then a higher standard applies: the Minister may authorise the interception if:
 - o the requirements of section 24 are met; and
 - o the conduct would also constitute a serious offence in Irish law and would justify the giving of a ministerial authorisation under domestic law.¹⁸³
- Where the person is in Ireland, the Minister also may make the authorisation and use of the intercepted messages subject to any condition that would apply if the authorisation had been granted in a domestic context.¹⁸⁴

These authorisations are deemed to be authorisations under the Interception of Postal Packets and Telecommunications (Regulation) Act 1993 – that is to say, this type of interception is an application of the domestic interception regime rather than an entirely new power.¹⁸⁵ This has two significant consequences. First, the limitations of the existing domestic regime apply in the context of interception on foot of a request from another member state. This means that interception under the Criminal Justice (Mutual Assistance) Act 2008 is not available in respect of any providers other than ‘authorised undertakings’, excluding over-the-top communications services.¹⁸⁶ Second, these interceptions also come within the scope of the Complaints Referee and designated judge oversight mechanisms under the 1993 Act.

12.5.3.5 Legal Remedies and Protection of Fundamental Rights

12.5.3.5.1 REFUSAL OF ASSISTANCE. Section 3(1)(b) of the Criminal Justice (Mutual Assistance) Act 2008 provides that requests for assistance under the Act shall be refused if

there are reasonable grounds for believing

- (i) that the request concerned was made for the purpose of prosecuting or punishing a person on account of his or her sex, race, religion, ethnic origin, nationality, language, political opinion or sexual orientation, [or]
- (ii) that providing assistance—

¹⁸² Criminal Justice (Mutual Assistance) Act 2008, ss. 25(1) and 25(2). Note that requests for immediate transmission are preferred, so requests for interception and recording followed by transmission of the recording can be authorised only if immediate transmission is not possible: s. 25(2).

¹⁸³ Ibid., s. 25(3).

¹⁸⁴ Ibid., s. 25(5).

¹⁸⁵ Ibid., s. 25(8).

¹⁸⁶ Council of the European Union, *Report on Ireland*, 104.

- (I) may prejudice a person's position for any of those reasons, or
- (II) may result in the person being subjected to torture or to any other contravention of the European Convention on Human Rights.

12.5.3.5.2 PURPOSE LIMITATION. There is a purpose limitation principle in the case of each of the statutory powers¹⁸⁷ to take evidence and search for data in response to inbound requests: an assurance must be given by the requesting authority (a) that any evidence supplied in response to the request will not, without the Minister's prior consent, be used for any purpose other than that permitted by the relevant international instrument or specified in the request, and (b) that the evidence will be returned when no longer required for that purpose¹⁸⁸ unless the Minister indicates that its return is not required.¹⁸⁹

12.5.3.5.3 NOTIFICATION. There is no statutory provision for notification of individuals that their data is to be accessed (or has been accessed) under mutual assistance procedures. This has been unsuccessfully challenged on fair procedure grounds in the past; in *Brady v. Haughton*,¹⁹⁰ the Supreme Court considered the power to take evidence for mutual assistance under section 51 of the Criminal Justice Act 1994¹⁹¹ and held that it was not unconstitutional by permitting evidence to be taken without notice to a party who may be affected. Instead, the majority in the Supreme Court described the procedure as an evidence-gathering exercise that would not give rise to an entitlement to be informed under domestic law.¹⁹²

Whether or not there is notification will, therefore, depend on the policy of the provider. A problem in this regard is that section 100 of the Criminal Justice (Mutual Assistance) Act 2008 creates a very wide 'tipping-off' offence carrying a possible penalty of five years' imprisonment: 'Where a request¹⁹³ is made in connection with a criminal investigation in the State or a designated state, any person who, knowing or suspecting that the investigation is taking place, makes any disclosure which is likely to prejudice the investigation is guilty of an offence.' This offence does not require any intention to prejudice the investigation, merely knowledge or suspicion that an investigation is taking place. It is a defence for the defendant to prove that they '(a) did not know or suspect that the disclosure to which the proceedings relate was likely to prejudice the investigation concerned, or (b) had lawful authority or reasonable excuse for making the disclosure'. The term 'reasonable excuse' is not defined in the legislation, making it difficult for a provider to know whether it would be committing an offence by notifying a user of a mutual assistance request in accordance with its general policy.

¹⁸⁷ Criminal Justice (Mutual Assistance) Act 2008, ss. 63, 74 and 75.

¹⁸⁸ Or any other purpose for which such consent has been given.

¹⁸⁹ In the context of e-evidence, the obligation to return makes less sense but might be interpreted as an obligation to delete the local copy.

¹⁹⁰ *Brady v. Haughton* [2006] 1 IR 1.

¹⁹¹ The precursor to section 63 of the Criminal Justice (Mutual Assistance) Act 2008.

¹⁹² The position may be different in relation to particularly sensitive types of information: in *Brady v. Haughton* itself, a number of the judges expressed concern about access to medical records without notice, and in *Burns v. O'Neill* [2015] IEHC 553, *LK v. Minister for Justice and Equality* [2016] IECA 361 and *LK v. Minister for Justice and Equality* [2016] IECA 362, the state accepted that it was obliged to notify individuals where their medical records were sought. It is arguable that the same principle should apply in respect of telecommunications records; for the time being, however, there is no notification in this context.

¹⁹³ Defined as 'a request for assistance which is made by a requesting authority under and in accordance with a relevant international instrument'. Criminal Justice (Mutual Assistance) Act 2008, s. 2.

12.5.3.5.4 DUTY OF DISTRICT COURT JUDGE TO CONSIDER PRIVACY RIGHTS. The privacy rights of an individual when evidence is sought for mutual assistance have been considered in *LK v. Minister for Justice and Equality*.¹⁹⁴ That case involved a letter of request from the UK for medical records concerning LK, who was to be a witness in a murder trial; the records were sought by the defendant with a view to discrediting her testimony. Her treating doctor and representatives from a hospital and another medical body were summoned to appear before a nominated District Court judge with the relevant records. Having been told that LK was vehemently opposed to the release of her information, each of them was legally represented and asserted, on her behalf, that the records were not compellable. This argument was rejected by the judge who found that production of the records could be compelled, notwithstanding that this form of third-party discovery would not be available in a domestic criminal matter.

Subsequently, LK brought a judicial review of that decision, and the Court of Appeal quashed the order to produce the evidence on the basis that the judge had erred by failing to consider her privacy rights under the Constitution and under Article 8 ECHR. *Per* Edwards J., where a District Court judge is nominated to take evidence relating to an individual, they are under an obligation ‘to have regard to, and to take into account, the [individual’s privacy rights] even if they had not been expressly asserted either by the [individual] or by an advocate putting forward a case on [their] behalf’,¹⁹⁵ and in doing so must balance the rights of the individual against other considerations ‘such as the public interest and the exigencies of the common good, and indeed the right of the defendant in the requesting state to receive a fair trial’.¹⁹⁶

12.5.3.5.5 VOLUNTARY COOPERATION. We have already seen (in Section 12.4.3) how providers in Ireland developed a practice of voluntary disclosure of user data to police,¹⁹⁷ relying on section 8 of the Data Protection Acts 1988 and 2003. This extends to requests from law enforcement agencies in other jurisdictions – making Ireland, according to the Commission, the only jurisdiction in the EU to permit this.¹⁹⁸

What is, perhaps, most striking about the cross-border nature of this practice is how little attention it has received. What is the legal basis for the provider to make voluntary disclosure to foreign law enforcement – particularly where the transfer is outside the EEA and bypasses the safeguards established by the existing mutual legal assistance framework?

There is almost no public information about this, apart from what emerged during Facebook’s 2011 audit by the Data Protection Commissioner. During that audit Facebook argued that international disclosure of non-content data – worldwide, not just within the EEA – was permissible on the basis that either:

- the exception in section 8(b) of the Data Protection Acts 1988 and 2003 for ‘preventing, detecting or investigating offences, apprehending or prosecuting offenders’ permitted disclosure for foreign criminal investigations; or
- users consented to such disclosure through the Privacy Policy; or

¹⁹⁴ See *LK v. Minister for Justice and Equality* [2016] IECA 361 and [2016] IECA 362. While this case deals with section 63 of the Criminal Justice (Mutual Assistance) Act 2008 regarding the taking of evidence before a court, the same principles should apply regarding searches for evidence under sections 74 and 75 so that an order under those sections could also be quashed if it failed to take into account the privacy interests involved.

¹⁹⁵ See *LK v. Minister for Justice and Equality* [2016] IECA 362, para. 23.

¹⁹⁶ See *LK v. Minister for Justice and Equality* [2016] IECA 362, para. 24.

¹⁹⁷ See, e.g., McIntyre, ‘Voluntary Disclosure of Data to Law Enforcement’.

¹⁹⁸ See, e.g., Commission of the European Communities, *Non-paper*, 1, 3–4.

- disclosure to other jurisdictions was lawful in light of Facebook's legitimate interest in cooperating with law enforcement authorities.¹⁹⁹

A full assessment of these arguments is outside the scope of this chapter, but there were question marks over them even then. For example, the reliance on section 8(b) to permit disclosure to foreign agencies was misconceived, as this section applied only to offences and court orders enforceable under Irish law.²⁰⁰ Similarly, Facebook's argument that users consent to data being transferred for criminal investigations was a questionable application of consent under Directive 95/46/EC, and is now unsustainable in light of the heightened standard of consent in Article 7 GDPR.²⁰¹

The lack of transparency in this area makes it difficult to assess, but in principle voluntary disclosures within the EEA might be permissible on the same conditions as domestic disclosures, discussed earlier in Section 12.4.3. The additional question that arises in the cross-border context is whether a voluntary disclosure for law enforcement purposes can be made to a third country in a way that is compatible with Chapter V of the GDPR.

It is difficult to see how these voluntary disclosures to third countries for law enforcement purposes could be legitimated. None of the relevant Article 49 GDPR derogations would appear to be available. User 'consent' in terms of use would not meet the requirements of prior information and explicit consent under Article 49(1)(a) GDPR. The Article 49(1)(e) derogation for transfers 'necessary for the establishment, exercise or defence of legal claims' appears to be limited to cases in which the data controller is closely involved rather than cases where the controller merely holds some evidence;²⁰² but, even on a wider interpretation, transfers for merely *investigative* purposes would not fall within the derogation.²⁰³ The 'important reasons of public interest criterion' under Article 49(1)(d) will not apply where the public interest at stake is that of a third country; the European Data Protection Board (EDPB) has stressed that it is available only where 'it can also be deduced from EU law or the law of the member state to which the controller is subject that such data transfers are allowed for important public interest purposes including in the spirit of reciprocity for international cooperation'.²⁰⁴ As a result, the EDPB has issued guidance: 'In situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to [the] existing MLAT or agreement.'²⁰⁵ In light of this, the practice of voluntary disclosure to non-EEA law enforcement agencies is of questionable legality at best.

12.5.4 Opportunities and Challenges Created by the e-Evidence Regulation

In a notable change from a previous policy of opting out of the EIO and other instruments, Ireland has opted into the new e-Evidence Regulation.²⁰⁶ This is particularly significant owing to

¹⁹⁹ See, e.g., Data Protection Commissioner, *Facebook Ireland Report of Audit*, appendix 5.

²⁰⁰ Annette Hogan, 'The Interception of Communications in Ireland: Time for a Re-Think' (2014) 7(5) *Data Protection Ireland* 8.

²⁰¹ See, e.g., Haase and Peters, 'Ubiquitous Computing and Increasing Engagement', 131–132.

²⁰² European Data Protection Board (EDPB), *Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679* (25 May 2018), 11, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.

²⁰³ Kopp and Pfisterer, 'Between a Rock and a Hard Place', 73; EDPB, *Guidelines 2/2018*, 11.

²⁰⁴ EDPB, *Guidelines 2/2018*, 10.

²⁰⁵ *Ibid.*, 5.

²⁰⁶ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191.

the presence of many service provider European headquarters in Ireland. Recognising the perception of Ireland as a weak regulator, an internal government memorandum noted: “There is already a perception in some member states that Ireland is benefitting financially by attracting such international service providers to establish themselves in Ireland but is not willing to properly regulate them, to the detriment of other EU states ... Non-participation in the e-evidence proposal will strengthen that view.”²⁰⁷

The Regulation entered into force in August 2023, but it will be three years before all aspects of the Regulation fully apply. The extent of the Regulation’s implications for Irish practice will become apparent over time, but a few observations can be made at this point. From a fundamental rights perspective, the starting point is that Irish law is in need of significant reform. For example, as we have seen in Sections 12.4.3 and 12.4.5, the lack of notification for users whose data has been accessed²⁰⁸ and the heavy reliance on voluntary disclosure of data mean that there are key gaps in regulation. In principle, the e-Evidence Regulation offers an opportunity to remedy these problems – for example, it will introduce independent approval for access to traffic and content data, which at the moment can be accessed by voluntary cooperation without any judicial control. Consequently, aspects of the package would represent a significant improvement on the Irish legal framework. Against that, however, the Regulation will do nothing to enhance the legal certainty or protection of fundamental rights if it becomes simply an additional layer that leaves the existing legal instruments and voluntary cooperation practices in place underneath.

Specific challenges to the operation of the Regulation’s safeguards may arise in Ireland owing to the high number of service providers headquartered in the state. The Regulation’s reliance on a notification process²⁰⁹ – where the enforcing authority in the service provider’s country of establishment has only ten days (ninety-six hours in an emergency) to raise a ground for refusal of a production order – clearly prioritises efficiency.²¹⁰ Considering the outsized number of requests likely to be received by the competent Irish authority and the short time limits to raise a ground for refusal, the ability of the enforcing authority notification requirement to provide effective protection remains in question.²¹¹

From the perspective of providers, the Regulation also significantly increases their burdens. For example, the requirement that in emergency cases data must be transmitted within eight hours has no parallel under existing Irish law, which usually gives providers seven days to comply with a mandatory order to disclose data.²¹² The sanctions for failure to provide information – up to 2 per cent of worldwide annual turnover – are several orders of magnitude greater, and are exacerbated by the limited grounds on which a disclosure requirement can be challenged.²¹³ At the moment providers based in Ireland typically have a ‘reasonable excuse’ defence for failure to comply with an interception warrant, search warrant or production order; the Regulation, by taking a ‘de facto impossibility’ approach, will make it more difficult to defend a failure to provide data based on issues of technical difficulty or conflicting legal obligations.²¹⁴

²⁰⁷ Fiach Kelly, ‘Government Told to “Properly Regulate” Internet Giants’, *Irish Times*, 9 July 2018, www.irishtimes.com/news/ireland/irish-news/government-told-to-properly-regulate-internet-giants-1.3558281.

²⁰⁸ Except in relation to Schedule 2 data under the Communications (Retention of Data) Act 2011.

²⁰⁹ Reg. 2023/1543, Art. 8.

²¹⁰ Ibid., Art. 12.

²¹¹ Valerie Albus, ‘Fast-Tracking Law Enforcement at the Expense of Fundamental Rights’, *Verfassungsblog*, 15 June 2023, <https://verfassungsblog.de/fast-tracking-law-enforcement-at-the-expense-of-fundamental-rights/>.

²¹² Reg. 2023/1543, Art. 10; Francisco and Rosenkranz, ‘United States of America v. Microsoft Corporation’, 37.

²¹³ Reg. 2023/1543, Art. 15.

²¹⁴ Ibid., Arts. 16(4)(c) and 16(5)(b). The risk of legal conflicts is partially mitigated by the review procedure in the event of conflicting obligations set out in Article 17. The Regulation also makes reference to denying an order on the basis

Finally, it is not clear that the Regulation itself will significantly improve the position for Irish law enforcement. It is limited to cross-border cooperation, with production and preservation requests to domestic service providers still being subject to national law. With many of the main internet firms having their Europe, Middle East and Africa (EMEA) headquarters in Ireland, Irish police may not get much practical benefit from the Regulation; national law, with all the problems outlined already, would still be more important. In addition, the Regulation does nothing to address the problem of admissibility, so that police in Ireland may end up with faster access to material for investigative purposes but continue to face issues in using that material for prosecution purposes. Consequently, it will be important to see how far domestic implementing legislation goes beyond the Regulation itself. At the time of writing (February 2024), proposed legislation to implement the Regulation has just been published and is about to enter pre-legislative scrutiny.²¹⁵

12.6 CONCLUSION

The issue of access to digital evidence is of fundamental importance in Ireland, but the dated legal framework, the lack of adequate oversight and the lack of transparency around the activities of the Irish authorities and providers with an Irish presence make it difficult to assess Irish law in this area. Where we do have detailed information on how access to data operates in practice – from the Facebook audit and the Murray report – it has been the result of ad hoc investigations into particular scandals. But the material that is publicly available makes it clear that reform of the law on access to data is long overdue. Between the invalidation of data retention, the need for modernisation of interception and the e-Evidence Regulation, there is pressure from all directions on the existing framework.

Despite these factors, the state has largely failed to act. The Department of Justice has yet to present any coherent plan to modernise Irish law. Instead, the strategy to date has been one of kicking the can down the road. This failure would be notable even if its effect were merely domestic, but it is magnified by the fact that it also impacts hundreds of millions of users elsewhere whose data is stored and managed in Ireland. By encouraging internet firms to establish in Ireland, the state has taken on a responsibility to properly regulate access to the data of their users – and that responsibility is not being met. Without a transparent reform process that respects the European privacy and data protection framework, Irish law will continue to fail both the protection of fundamental rights and the public interest in effective investigation of crime.

of ‘immunities or privileges granted under the law of the enforcing State, or [where] the data requested are covered by rules on the determination or limitation of criminal liability that relate to freedom of the press or freedom of expression in other media’ and provision for denial in ‘exceptional situations’ where it is apparent that there are substantial grounds to believe, ‘on the basis of specific and objective evidence’, that the execution of the order would entail a ‘manifest breach of a relevant fundamental right as set out in Article 6 TEU and the Charter’ (Reg. 2023/1543, Arts. 16(4)(f)–(g) and (5)(e)–(f)).

²¹⁵ Department of Justice, ‘Ministers McEntee and Browne Receive Approval to Draft Legislation to Allow Gardai Swift Access to Digital Criminal Evidence’, 7 February 2024, www.gov.ie/en/press-release/81d45-ministers-mcentee-and-browne-receive-approval-to-draft-legislation-to-allow-gardai-swift-access-to-digital-criminal-evidence/.

Digital Evidence and the Cooperation of Service Providers in Luxembourg

Katalin Ligeti and Gavin Robinson

13.1 INTRODUCTION

Luxembourg sits near the top of several regional and international indexes for information and communication technology (ICT) development, digital economy and society, and technological readiness,¹ and hosts an impressive and growing number of data centres along with the regional or global headquarters of major internet and e-commerce players including Amazon and PayPal (both European HQ)² and Viber (global HQ). The favourable economic environment attracting such market leaders harnesses, inter alia, Luxembourg's powerful finance industry in need of high-performance technologies, its geographical location in the heart of Western Europe and a diverse, multilingual and highly skilled workforce.³

Although targeted official statistics are not compiled, our interview-based research indicates that Luxembourg's small size, highly connected nature and financial strength translate into the active cooperation of service providers (SPs) in criminal investigations in both domestic and cross-border situations.⁴ A discrepancy is observed regarding the legal frameworks applicable, first, to the cooperation of domestic SPs (having a physical presence in Luxembourg) with Luxembourg law enforcement authorities (LEAs); second, to the cooperation of domestic SPs with foreign LEAs; and third, to the cooperation of SPs based outside Luxembourg with Luxembourg LEAs. While the domestic configuration benefits from a rather complete legal framework, the two other configurations lack specific provisions that could allow for a clear definition of the duties of SPs and the rights of data subjects.

Depending on the type of service provider, the type of data sought and the applicable legal basis, the cooperation may be voluntary, de facto mandatory as a corollary of being regulated, or de iure mandatory – but with the emphasis firmly on the last scenario, that is, via binding duties set out in the Luxembourg Code of Criminal Procedure (CCP).⁵

This chapter aims to provide an overview of the Luxembourg legal framework and of the challenges relating to the various forms of cooperation between SPs and LEAs for an

¹ L. Funck, 'Luxembourg', in M. T. Murchison (ed.), *The Technology, Media and Telecommunications Review*, 13th ed. (London: Law Business Research, 2022), 179.

² Until September 2019, Skype's European HQ was also in Luxembourg.

³ Funck, 'Luxembourg', 180.

⁴ The interviews were conducted between 2019 and 2022. The interviewees were judges, police officers, representatives of the prosecutor's office, representatives of service providers established in Luxembourg and a data protection expert.

⁵ Code de procédure pénale (Luxembourg Code of Criminal Procedure as amended, CCP), originally enacted as the Code d'instruction criminelle, Mémorial A214, 17 November 1808, Arts. 48-27, 67-1 and 88-4.

international audience not necessarily familiar with the Luxembourg legal system. Luxembourg law, along with the vast majority of the legal literature, is in French: except where indicated, all translations hereinafter are the authors' own.

13.2 SETTING THE SCENE

13.2.1 *General Approach to the Collection of Digital Evidence*

To a large extent, in Luxembourg, the collection of digital evidence is carried out on the basis of existing horizontal measures in the CCP, wherein the figure of the investigating judge (*juge d'instruction*) and their coercive powers remain central. In the places where the legal framework has been adapted to the specificities of electronic data and digital evidence, the impetus to do so has most often come from a need to keep pace with developments either in neighbouring jurisdictions or at the EU or international level rather than internal initiatives.⁶ Furthermore, at least as far as cooperation with SPs is concerned, modifications of the legal framework tend to be characterised as clarifications or refinements of powers which are already in place (or used in practice) rather than as any grand revision or overhaul.

The implementation of the Budapest Convention is a good example of this trend.⁷ The Convention was implemented in Luxembourg law by the Law of 18 July 2014.⁸ As the substantive criminal offences set out in the Convention were already essentially covered in Articles 509-1 to 509-7 of the Luxembourg Criminal Code,⁹ the main added value of the implementing law is in matters of criminal procedure,¹⁰ including notably the introduction of rapid preservation of data (quick freeze). Seizure of electronic data was reportedly already being carried out on the basis of general seizure provisions – despite their clear emphasis on physical objects – and as such the Budapest reform added a measure of legal certainty to the process of seizing digital evidence without tackling the questions of ensuring its authenticity and integrity.¹¹ Departing from the general regime on the collection of evidence, in the sense that it provides for specific baseline

⁶ The introduction into Luxembourg law of cyber infiltration and undercover investigation is one example. Indeed, the regime of those investigatory tools has drawn inspiration from the practice in France and Belgium as well as from recommendations of the Council of Europe. See Exposé des motifs, Projet de loi n° 6921 adaptant la procédure pénale aux besoins liés à la menace terroriste et portant modification (1) du Code de procédure pénale, (2) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, (3) de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques (Explanatory Statement of Bill 6921), 8 March 2016, p. 7; see also Council of the EU, Report on Luxembourg (7162/1/17), 7th Round of Mutual Evaluations: The Practical Implementation and Operation of European Policies on Prevention and Combating Cybercrime (Outcomes of the Council GENVAL Evaluations 2017), 19 May 2017, <http://data.consilium.europa.eu/doc/document/ST-7162-2017-REV-1-DCL-1/en/pdf>, p. 99 (stating that 'Luxembourg should reflect on adopting technical and legal tools to carry out infiltration operations and undercover investigations in cyberspace').

⁷ Council of Europe, Convention on Cybercrime, ETS No. 185, 23 November 2001.

⁸ Loi du 18 juillet 2014 portant (1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001, (2) approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003, (3) modification du Code pénal, (4) modification du Code d'instruction criminelle, (5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques (Law Implementing the Budapest Convention), 18 July 2014, Mémorial A133, 25 August 2014.

⁹ Those provisions are part of section VII 'De certaines infractions en matière informatique' of the CCP.

¹⁰ M. Braun, 'La ratification de la Convention de Budapest sur la cybercriminalité par le Luxembourg' (2014) 35 *Journal des tribunaux Luxembourg* 121–133.

¹¹ CCP, Arts. 31 and 33. See further K. Ligeti and G. Robinson, 'The Handling of Digital Evidence in Luxembourg', in M. Caianiello and A. Camon (eds.), *Digital Forensic Evidence: Towards Common European Standards in Antifraud Administrative and Criminal Investigations* (Milan: Wolters Kluwer, 2021), 123–163.

procedures, the 2014 law implementing the Budapest Convention has introduced such procedures for the seizure of stored content data by the investigating judge in the course of a judicial inquiry or the public prosecutor in the limited *mini-instruction* scenario.¹² These – modest – adjustments include an express provision on the making of copies – rather than the seizure of physical electronic devices – and the enlisting of decryption experts. In practice, it appears that when a copy of seized data is made, the data used as evidence is simply saved on a CD, DVD, hard drive or USB stick depending on the volume of data to be seized.¹³

Additionally, the impact of the Law Enforcement Directive (LED) via the Law of 1 August 2018 is still keenly awaited.¹⁴ The law sets out the fundamental data protection principles that police and judicial actors engaged in the obtaining and managing of digital evidence will have to respect while doing so, such as the principles of purpose limitation,

¹² The so-called *mini-instruction* is a simplified procedure that exceptionally allows for the seizure of data without conducting a preliminary investigation liable to corroborate the culpability of the suspect. This procedure initially applied to misdemeanours related to money laundering or funding of terrorism but has been extended to also cover misdemeanours punishable with a maximum term of imprisonment of at least one year (Law Implementing the Budapest Convention). During such a procedure, telecommunication service providers are bound to cooperate with the investigating judge by providing the requested data. This remains unaltered by the introduction of several procedural safeguards aiming to guarantee the protection of the rights of the suspect in the Loi du 8 mars 2017 renforçant les garanties procédurales en matière pénale portant: transposition de la directive 2010/64/UE du 20 octobre 2010 relative au droit à l'interprétation et à la traduction dans le cadre des procédures pénales; transposition de la directive 2012/13/UE du 22 mai 2012 relative au droit à l'information dans le cadre des procédures pénales; transposition de la directive 2013/48/UE du 22 octobre 2013 relative au droit d'accès à un avocat dans le cadre des procédures pénales et des procédures relatives au mandat d'arrêt européen, au droit d'informer un tiers dès la privation de liberté et au droit des personnes privées de liberté de communiquer avec des tiers et avec les autorités consulaires; transposition de la directive 2012/29/UE du 25 octobre 2012 établissant des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité; changement de l'intitulé du Code d'instruction criminelle en 'Code de procédure pénale'; modification: du Code de procédure pénale; du Code pénal; de la loi du 7 juillet 1971 portant en matière répressive et administrative, institution d'experts, de traducteurs et d'interprètes assermentés; de la loi modifiée du 10 août 1991 sur la profession d'avocat; de la loi modifiée du 20 juin 2001 sur l'extradition; de la loi modifiée du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres de l'Union européenne (Law on Procedural Safeguards in Criminal Proceedings), 8 March 2017, Mémorial A346, 30 March 2017.

¹³ Interview with a Luxembourg investigating judge, December 2022. See also Council of the EU, Report on Luxembourg, 52, and Ligeti and Robinson, 'The Handling of Digital Evidence in Luxembourg', 130.

¹⁴ Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et portant modification 1° de la loi modifiée du 7 mars 1980 sur l'organisation judiciaire; 2° de la loi modifiée du 29 mai 1998 portant approbation de la Convention sur la base de l'article K.3 du Traité sur l'Union européenne portant création d'un Office européen de police (Convention Europol), signée à Bruxelles, le 26 juillet 1995; 3° de la loi du 20 décembre 2002 portant approbation – de la Convention établie sur base de l'article K.3 du Traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, signé à Bruxelles, le 26 juillet 1995; – de l'Accord relatif à l'application provisoire entre certains États membres de l'Union européenne de la Convention établie sur base de l'article K.3 du Traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, signé à Bruxelles, le 26 juillet 1995; 4° de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité; 5° de la loi modifiée du 16 juin 2004 portant réorganisation du centre socio-éducatif de l'État; 6° de la loi modifiée du 25 août 2006 relative aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle; 7° de la loi du 24 juin 2008 ayant pour objet le contrôle des voyageurs dans les établissements d'hébergement; 8° de la loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire; 9° de la loi modifiée du 19 décembre 2014 facilitant l'échange transfrontalier d'informations concernant les infractions en matière de sécurité routière; 10° de la loi modifiée du 25 juillet 2015 portant création du système de contrôle et de sanction automatisés; 11° de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État; 12° de la loi du 23 juillet 2016 portant mise en place d'un statut spécifique pour certaines données à caractère personnel traitées par le Service de renseignement de l'État; 13° de la loi du 22 février 2018 relative à l'échange de données à caractère personnel et d'informations en matière policière; 14° de la loi du 18 juillet 2018 sur la Police grand-ducale; et 15° de la loi du 18 juillet 2018 sur l'Inspection générale de la Police (LED Law), 1 August 2018, Mémorial A689, 16 August 2018.

adequacy, accuracy, data minimisation and data security, along with a suite of data subject rights (e.g. right to information, right of access, rights to rectification and erasure) for the person(s) concerned, and logging and documentation requirements for data controllers.¹⁵ Transparency ought to be further improved by the monitoring of compliance of judicial processing of personal data with the LED rules by a new ‘Judicial Control Authority’ (*Autorité de contrôle judiciaire*),¹⁶ composed of representatives of the highest courts and prosecutors along with a representative of the national data protection authority, the National Commission for Data Protection (*Commission nationale pour la protection des données* – CNPD).¹⁷ In consultation with our research team in late 2022, a member of the CNPD observed that the impact of the transposition of the LED in Luxembourg law is significant, in that it is forcing law enforcement to rethink its processing of personal data, including sensitive data. From an organisational perspective, the member noted, LEAs are ‘building an entire data governance’ to comply with the LED.

From an operational perspective, in 2017 the ‘New Technologies’ section of Luxembourg’s Grand-Ducal Police was cited – in the cybercrime context – as an example to the rest of Europe with regard to its composition, its tasks and its positioning at the international level. In particular, the possibility for civilian information technology (IT) experts to qualify as officers of the judicial police was adjudged to enable a fruitful rapprochement of skills, which Council of Europe evaluators put forward for development at the European level.¹⁸

13.2.2 Data Retention Obligations: Legal Framework, Practice and Challenges

There are two relevant obligations relating to data retention in Luxembourg law. The first is the retention of traffic and location data by communications service providers.¹⁹ The second is the retention of clients’ subscriber and identification data by providers of number-based interpersonal communications services (such as prepaid subscriber identity module (SIM) plans).²⁰ Relatedly, there is also the daily feeding by regulated electronic communication services (ECS) providers of usage and subscriber data into a register operated by the regulator (*Institut*

¹⁵ See LED Law, Art. 3.

¹⁶ See LED Law, ch. 6, s. 2.

¹⁷ This Commission is governed by the Loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d’avancement des fonctionnaires de l’État (CNPD Law), 1 August 2018, Mémorial A686, 16 August 2018. An overview of the missions of the authority of judicial control is available on the CNPD website: <https://cnpd.public.lu/fr/commission-nationale/Autorite-contrôle-judiciaire.html>.

¹⁸ Council of the EU, Report on Luxembourg, p. 33.

¹⁹ Loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l’égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification des articles 88–2 et 88–4 du Code d’instruction criminelle (2005 Law on the Protection of Private Life), 30 March 2005, Mémorial A73, 7 June 2005, as modified by Loi du 24 juillet 2010 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l’article 67–1 du Code d’instruction criminelle (2010 Law on the Protection of Private Life), 24 July 2010, Mémorial A122, 29 July 2010, Arts. 5 and 9.

²⁰ Loi du 17 décembre 2021 portant transposition de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen et portant modification de la loi modifiée du 30 mai 2005 portant: (1) organisation de l’Institut Luxembourgeois de Régulation; (2) modification de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l’État (EEC Code Law), 17 December 2021, Mémorial A927, 22 December 2021. Art. 116. Subscriber and identification data of clients of electronic communication service providers must be retained for the duration of the business relationship, plus three years thereafter.

Luxembourgeois de Régulation; ILR) for access by competent authorities in the context of criminal proceedings (as well as intelligence operations).²¹

To begin with the first obligation just introduced, the Data Retention Directive (DRD)²² was implemented in Luxembourg by the 2010 Law on the Protection of Private Life, amending Articles 5 and 9 of the 2005 Law on the Protection of Private Life, which had itself implemented the e-Privacy Directive.²³ The 2005 Law had already established a national data retention scheme on the basis of Article 15(1) of the e-Privacy Directive, before the 2010 Law subsequently aligned that scheme with the provisions of the DRD, in the process reducing the retention period from twelve months to the DRD minimum of six months,²⁴ corresponding to the average length of criminal proceedings in Luxembourg. Furthermore, the 2010 Law limited LEA access to data retained by SPs to criminal offences that are punishable with at least one year's imprisonment.²⁵

In the wake of the Court of Justice of the European Union's (CJEU's) annulment of the DRD in *Digital Rights Ireland*,²⁶ the Luxembourg Ministry of Justice moved quickly to propose a recalibration of domestic data retention provisions via Bill 6763, released in January 2015.²⁷ In this case, the country bucked a trend insofar as the impulse to accommodate the CJEU judgment in national law came from the government – as opposed to (constitutional) court challenges driven by fundamental rights non-governmental organisations, as has occurred in several other member states.²⁸ The planned reform was to (i) tighten access to retained data to an exhaustive list of defined criminal offences carrying a maximum sentence of at least one year's imprisonment; (ii) tighten existing requirements to delete data at the end of the retention period; (iii) increase the length of prison terms for non-compliance; and (iv) stipulate that data must be retained within the territory of the European Union. The option of a three-month retention period was also raised before the Parliament, with the Ministry of Justice and the Public Prosecutor defending a six-month limit by reference to the average length of criminal proceedings.

²¹ Loi du 27 juin 2018 adaptant la procédure pénale aux besoins liés à la menace terroriste et portant modification (1) du Code de procédure pénale, (2) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, (3) de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques (Law on Terrorist Threats), 27 June 2018, Mémorial A559, 5 July 2018, Arts. 2–4.

²² Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, [2006] OJ L105, 13 April 2006.

²³ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications, e-Privacy Directive), [2002] OJ L201, 31 July 2002.

²⁴ First reduced from twelve months in relation to traffic data by Loi du 27 juillet 2007 portant modification de la loi loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel; des articles 4 paragraphe (3) lettre d); 5 paragraphe (1) lettre a); 9 paragraphe (1) lettre a) et 12 de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 23 paragraphe (2) points 1. et 2. de la loi du 8 juin 2004 sur la liberté d'expression dans les medias, 27 July 2007, Mémorial A131, 8 August 2007, Art. 33, before the 2010 Law on the Protection of Private Life (n. 19) made the same reduction for location data other than traffic data; Art. 1(3).

²⁵ See the 2005 Law on the Protection of Private Life, Arts. 5(1) and 9(1), as amended by the 2010 Law on the Protection of Private Life, Art.1(1) and 1(3).

²⁶ Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:38.

²⁷ Projet de Loi n° 6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques (Bill 6763), 7 January 2015.

²⁸ Singling out the government's initiative and comparing national responses to CJEU jurisprudence on data retention across the EU. See Privacy International, 'National Data Retention Laws since the CJEU's Tele-2/Watson Judgment', September 2017, p. 12, https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf. The lack of a judgment ruling the 2010 data retention regime as unconstitutional can also explain why the latter is still applicable.

However, these discussions were inconclusive before the *Tele2/Watson* judgment arrived in December 2016, solidifying the Court's stance that no degree of substantive or procedural restrictions could render the generalised and indiscriminate retention of all traffic and location data compatible with the Charter.²⁹ A full two years later, in December 2018 (following national elections in October 2018), the dossier was sent back to the competent Parliamentary commission, before a fresh Bill eventually emerged in January 2023.³⁰ The Bill will be discussed a little later in this section; at the time of writing, the data retention provisions in Luxembourg law remain essentially in their 2010 state.

Accordingly, operators of public communications networks and providers of ECS which are accessible to the public over such networks must retain traffic data (Article 5 of the Law on the Protection of Private Life) and location data other than traffic data (Article 9 of the Law on the Protection of Private Life) for a period of six months.³¹ Upon expiry of the retention period, both types of data must be erased or rendered anonymous.³² Since, for ECS, the personal scope of the data retention obligations is tied to the definition of that term in the 2005 Law on the Protection of Private Life, providers of what were long known as 'information society services' (ISS) which 'do not consist wholly or mainly in the transmission of signals by means of electronic communications networks' are not subject to them.³³ That means, for instance, that ISS which host content are not covered.³⁴

The precise data types to be retained almost exactly mirror the provisions in the annulled DRD. Indeed, the Grand-Ducal Regulation of 24 July 2010, determining the data categories generated or processed in the context of providing electronic communication services, provides that the retention obligation applies to data concerning legal persons and natural persons but not to the content of communications, including information consulted while using an electronic communications network.³⁵ Summarised, Article 3 of the Regulation covers data required in order to:

- (a) trace and identify the source of a communication;
- (b) identify the destination of a communication;

²⁹ Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen, and Secretary of State for the Home Department v. Tom Watson and Others* [2016] ECLI:EU:C:2016:970.

³⁰ Luxembourg Government, 'Sam Tanson Presented the Draft Law on the Retention of Personal Data', 25 January 2023, https://gouvernement.lu/en/actualites/toutes_actualites/communiqués/2023/01-janvier/25-tanson-loi-retention-donnees-caractere-personnel.html.

³¹ See 2005 Law on the Protection of Private Life, Art. 1.

³² 2005 Law on the Protection of Private Life, Arts. 5(1)(b) and 9(1)(b).

³³ The European Electronic Communications Code Directive was implemented in Luxembourg law by EEC Code Law, bringing some OTT service providers into the newly expanded definition of ECS for regulatory purposes. Such providers remain, however, exempted from any data retention obligation pursuant to the 2005 Law on the Protection of Private Life, Art. 2(k).

³⁴ In Luxembourg doctrine, it has nonetheless been argued that 'intermediary service providers', as defined in the Loi du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93 du 13 décembre 1999 relative à un cadre communautaire pour les signatures électroniques, la directive 2000/31/CE relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE du 20 mai 1997 concernant la vente à distance des biens et des services autres que les services financiers (2000 Law on e-Commerce), Mémorial A96, 8 September 2000, are subject to the data retention obligations in the modified 2005 law. See Braun, 'La ratification de la Convention de Budapest', 129. Observing that such an interpretation would be 'highly questionable' in the light of the clear legal framework, even if it would be more in line with the definition used in the Budapest Convention which includes '(i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and (ii) any other entity that processes or stores computer data on behalf of such communications service or users of such service', see V. Franssen and K. Ligeti, *The Cooperation of Internet and Other Service Providers with Judicial Authorities: National Report on Luxembourg*, 2015, 4, https://orbi.uliege.be/bitstream/2268/201353/1/Report_Luxembourg_Franssen%26Ligeti_Publication.pdf.

³⁵ See Règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de

- (c) identify the date, time and duration of a communication;
- (d) identify the type of communication;
- (e) identify users' communication equipment;
- (f) identify the location of the mobile communication equipment.³⁶

The above rules have thus remained in place as the CJEU has progressively broadened and deepened its data retention case law through such judgments as *La Quadrature du Net*,³⁷ *GD*³⁸ and *Spacenet*.³⁹ At the time of writing, it appeared that the admissibility of retained data as evidence in criminal proceedings in Luxembourg had not (yet) been affected by the CJEU's guidance on that facet of its case law.⁴⁰ Following Belgium's lead, Luxembourg now appears to have stopped waiting for the adoption of new common rules on data retention at EU level,⁴¹ and instead decided to push ahead with a national solution aiming to combine full respect of the CJEU's case law with law enforcement imperatives.

The Data Retention Bill proposes to insert a new Article 5bis in the 2005 Law on the Protection of Private Life, establishing the targeted retention of traffic and location data of users who find themselves (even for a moment, if mobile) in a designated geographical zone. In terms of crime, the retention mandate would cover geographical zones with higher risks of preparation and commission of acts of serious criminality, meaning:

- (a) areas (*lieux*) where crimes or *délits* punishable with a maximum term of imprisonment of at least one year are repeatedly committed;
- (b) areas (*lieux*) which, by their 'configuration', tend to encourage (*favoriser*) the commission of such offences;
- (c) the surroundings and limits of infrastructure where events of national or international stature (*envergure*) are regularly organised;
- (d) areas (*lieux*) which by their nature gather a large number of individuals.⁴²

An *Arrêté grand-ducal* (Grand-Ducal Decree) is set to calibrate the inner workings of 'targeted retention' as construed by the Luxembourg legislator.⁴³ That Decree, a joint product of the *Haut commissariat à la protection nationale* and a specially constituted consultative

communications publics (2010 Grand-Ducal Regulation), 24 July 2010, Mémorial A122, 29 July 2010, Art. 1, which reflects the DRD, Art. 5(2).

³⁶ The Luxembourg provision essentially copies DRD, Art. 5(1). Article 9(1)(a) of the 2005 Law on the Protection of Private Life also provides: 'For the purposes of this paragraph, only one piece of information on location (*information de localisation*) is required per communication or call.' As previously observed by Franssen and Ligeti, it is surprising to find records of unconnected calls explicitly excluded from data to be retained (Article 3(2) of the 2010 Grand Ducal Regulation), whereas both Article 3(2) of the DRD and Articles 5(1) and 9(1) of the 2005 law on the protection of private life include those data. See Franssen and Ligeti, *The Cooperation of Service Providers with Judicial Authorities*, 20.

³⁷ Case C-511/18, *La Quadrature du Net and Others* [2020] ECLI:EU:C:2020:791.

³⁸ Case C-140/20, *GD v. Commissioner of An Garda Síochána* [2022] ECLI:EU:C:2022:258.

³⁹ Joined cases C-793/19 and C-794/19, *SpaceNet AG & Telekom Deutschland GmbH* [2022] ECLI:EU:C:2022:702.

⁴⁰ Interview with a representative of the CNPD, December 2022.

⁴¹ See Luxembourg Government, Coalition Agreement 2018–2023, which stated 'it is urgent that the European Union adopt new common rules in conformity with the CJEU jurisprudence ... the national law will conform to the common European rules', p. 27, <https://gouvernement.lu/dam-assets/fr/publications/accord-coalition/2018-2023/Accord-de-coalition-2018-2023.pdf>.

⁴² *Projet de Loi n° 8148 relative à la rétention des données à caractère personnel et portant modification: 1 du Code de procédure pénale; 2 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques; et 3 de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat*, 8 February 2023 (Data Retention Bill), Art. 5bis(2).

⁴³ As with the current law, data categories are to be specified in a future *Règlement Grand-Ducal*; by contrast, however, the Bill expressly includes unsuccessful call attempts.

commission,⁴⁴ will draw the geographical perimeters of each of the above zones, renewable after evaluation every three years.

Turning now to another of the relevant obligations listed at the outset of this subsection, the Law on terrorist threats inserted an Article 10bis into the 2005 Law on the Protection of Private Life in order to further boost data-sharing by certain providers of ECS. The data is shared with the ILR via a central registry and is accessible, inter alia, by public prosecutors and investigating judges.⁴⁵ Service providers are obliged to transmit defined subscriber and usage data to the ILR for access by the competent authorities in the context of criminal proceedings or intelligence operations. The listed data must be updated at least once a day, even if there has been no change. Although not technically a measure of data *retention*, this constant data transfer appears to have comparable effects. Indeed, Article 10bis of the 2005 law, labelled ‘Centralised register within the Institute’, states that ECS providers which possess/use a Luxembourg dialling code shall:

(2) ... transmit automatically and free of charge to the Institute by electronic means and via a secure interface, the following data:

1. For natural persons: name, first name, habitual place of residence, date and place of birth along with the contact number of the subscriber;

For legal persons: denomination or business name (*raison sociale*), address of place of establishment along with a contact number;

2. The name of the regulated entity, the nature of the service provided by that entity, the call number allocated in relation to the service and, if available, the date of the end of the contractual relationship or in case of prepayment the deactivation date of the call number;
3. For natural persons, the type, the issuing country and the number of identification or proof of deposit of a request for international protection of the subscriber in cases of prepaid services.

Unlike the data retention obligations which refer to ‘traffic data’ and ‘location data other than traffic data’, no such *category* is referred to in the legislation creating a central register at the ILR. Regulatory sanctions apply to any provider who should fail to meet their obligations under the scheme. Regarding the legislative choice of creating a centralised register, it is worth noting that a provision capable of enabling such a set-up was included in the old national Data Protection Law from 2002,⁴⁶ now repealed by the General Data Protection Regulation (GDPR) and accompanying national legislation,⁴⁷ as well as by the implementation of the LED into national law.⁴⁸ Due to practical difficulties and the concomitant costs (at the time deemed ‘exorbitant and disproportionate to the aim pursued’),⁴⁹ the provision was reportedly never used before it was eventually repealed in 2011. Five years on, inspired by analogous developments in Belgian law, convinced of a ‘spectacular efficiency gain’ and no longer fazed by practical or resources obstacles, the Ministry of Justice proposed in the 2015 Bill to revive the provision in order to avoid

⁴⁴ Also to be defined in a future *Règlement Grand-Ducal*.

⁴⁵ Article 48-27 CCP also provides for a corollary cooperation duty on ‘telecommunications operators and telecommunications service providers’ to provide access for, inter alia, prosecutors, investigating judges or (in urgent cases and subject to strict limits) the police to data retained under Article 10bis of the 2005 Law on the protection of private life in order to identify subscribers, users or ECSs used.

⁴⁶ Loi du 2 août 2002 relative à la protection des personnes à l’égard du traitement des données à caractère personnel (2002 Data Protection Law), 2 August 2002, Mémorial A91, 13 August 2002, Art. 41.

⁴⁷ CNPD Law.

⁴⁸ LED Law.

⁴⁹ Explanatory statement of Bill 6921, p. 17. This Bill became the 2018 Law on Terrorist Threats.

having to either carry out searches at operators' premises (the status quo) or address orders (*réquisitions*) to operators. Direct, remote, electronic access to the relevant information was deemed necessary – and this in relation to all crimes and misdemeanours.⁵⁰

In any case since the *La Quadrature du Net* judgment,⁵¹ it is clear that 'civil identity data' can be *retained* generally and indiscriminately for the purpose of combating any crime or threat to public security, a fortiori serious crime or serious threats to public security (as well as national security). Therefore, the obligations imposed on certain ECS by the Law on Terrorist Threats to share with the ILR subscriber and usage data seem to follow this logic.

13.3 TERMINOLOGY AND CATEGORISATIONS

13.3.1 Data

13.3.1.1 Terminology

The term 'data' is not defined in any national law despite recurrent reference in the CCP to 'data stored, processed or transferred'.⁵² However, the directly applicable Article 4 of the GDPR offers a binding definition of 'personal data' that is also applicable within the scope of the LED law,⁵³ and that reads as follows:

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Furthermore, Article 9(1) of the GDPR provides a definition of 'special categories of personal data' ('sensitive data') that should be understood as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.

Luxembourg is part of the Council of Europe's 'Convention 108+',⁵⁴ which also defines in Articles 2(a) and 6 respectively the terms 'personal data'⁵⁵ and 'special categories of data'.⁵⁶ The lack of a national definition of 'data' does not seem to raise any particular issue when gathering data domestically or when cooperating with foreign authorities or SPs.

⁵⁰ Explanatory statement of Bill 6921, p.17. See Section 13.4.3 for the relevant provisions on access. Criminal offences in Luxembourg law are distinguished according to their gravity in three categories: minor offences (*contraventions*), misdemeanours and crimes.

⁵¹ *La Quadrature du Net and Others*.

⁵² CCP, Arts. 31, 33, 48-25 and 66.

⁵³ LED Law, Arts. 2(1)1 and 2(2).

⁵⁴ Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), ETS No. 223, 10 October 2018.

⁵⁵ 'Personal data' means any information relating to an identified or identifiable individual ('data subject').

⁵⁶ Genetic data; personal data relating to offences, criminal proceedings and convictions, and related security measures; biometric data uniquely identifying a person; personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life.

13.3.1.2 Categorisation

Nor is there any systematic categorisation of data types in Luxembourg law. Indeed, before the 2014 law implementing the Budapest Convention there was not even an express reference to data in national legislation concerning access by judicial authorities to information held by SPs. The general wording now enshrined in the seizure powers of the investigating judge pursuant to Article 66(1) of the CCP merely refers to ‘data stored, processed or transmitted in an automated data processing or transmission system’. Notably, the European Investigation Order (EIO) implementing law also makes no distinction between different categories of electronic data; it relies rather on the existing broadly termed powers in the CCP.⁵⁷

Fragments do exist elsewhere in the domestic legal framework: the categories of ‘traffic data’ and ‘location data other than traffic data’ that can be retained are inherited directly from the e-Privacy Directive⁵⁸ and are set out in the 2005 Law on the Protection of Private Life⁵⁹ as well as the Grand-Ducal Regulation of 24 July 2010.⁶⁰ The last of these excludes the retention of content data. Furthermore, the central register held by the ILR – which was established by the Law on Terrorist Threats – corresponds to subscriber and usage data, although this term is not used in the legislation which instead specifies the data to be forwarded to the register without ascribing a category or label to them. As will be presented in Section 13.4.3, a distinction between traffic, location and content data can be also found under the CCP in relation to the investigative measures involving data.

13.3.2 Service Providers

The general term ‘service provider’ (*fournisseur de services*) is used in several Luxembourg laws relating to telecommunications technologies and electronic services. However, depending on the legislation in question, the meaning of the term can differ. To a large extent, the differences are due to the European legal instruments underpinning the domestic provisions. In line with such instruments, Luxembourg law makes a distinction between providers of information society service(s) (ISS) and providers of electronic communication service(s) (ECS). The new terminology, ECS, reflects the increased scope of services and networks that are regulated, with express reference to internet services,⁶¹ as well as an attempt by the Luxembourg legislator to clarify as far as possible the types of providers concerned. However, the new terminology has not yet replaced the notion of ISS providers and continues to coexist with it, sometimes covering the very same type of service providers. The distinction between these two types of service providers is relevant in light of their obligations to retain certain data and cooperate with criminal investigations.

Articles 67-1 and 48-27 of the CCP, relating to the track and localise orders, and identification of a subscriber or common user, retain the old terminology which was used before the enactment of the 2011 Law on Electronic Communications Networks and Services, that is, providers of telecommunication service(s) (*fournisseur d'un service de télécommunications*).⁶² In the old

⁵⁷ Loi du 1er août 2018 portant 1° transposition de la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale; 2° modification du Code de procédure pénale; 3° modification de la loi modifiée du 8 août 2000 sur l'entraide judiciaire internationale en matière pénale (EIO Law), 1 August 2018, Mémorial A787, 11 September 2018.

⁵⁸ e-Privacy Directive, Art. 2(b) and (c). These terms were also found in the Data Retention Directive.

⁵⁹ 2005 Law on the Protection of Private Life, Art. 2(f) and (g).

⁶⁰ This Regulation provides the precise data types to be retained by electronic communication services providers (for more details, see Section 13.2.2).

⁶¹ Funck, ‘Luxembourg’, text to n. 46.

⁶² The Loi du 27 février 2011 sur les réseaux et les services de communications électroniques (2011 Law on Electronic Communications Networks and Services), 27 February 2011, Mémorial A43, 8 March 2011, repealed the Loi du 30

Telecommunications Law of 1997,⁶³ telecommunication was defined as ‘each transmission, emission or reception of signals, writings, images, sounds or data of any nature, by wire, radio, optical or electromagnetic means’.⁶⁴ Internet services were deemed to be covered by this definition.⁶⁵

The 2005 Law on the Protection of Private Life relating to the processing of personal data in the electronic communications sector applies to ‘the processing of ... personal data in the context of the provision of electronic communications services accessible to the public, on public communications networks’.⁶⁶ The same law defines a ‘service provider’ by reference to ECS. The latter is understood as a service provided against remuneration, consisting in the conveyance of signals and excluding editorial control over the transmitted content.⁶⁷ Also, the definition of ECS includes telecommunication services but excludes other ISS which do not consist in the conveyance of signals on electronic communication networks.⁶⁸

The ISS are defined in Article 1 of the 2000 Law on e-Commerce, implementing the e-Commerce Directive, as ‘any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services’. With respect to ISS, the term ‘service providers’ extends to any natural or legal person which provides internet access or merely transmits information on a communication network, which effects automatic, intermediate and temporary storage of such information (‘caching’; e.g. proxy servers) and which stores information provided by a recipient of the service (‘hosting’; e.g. Facebook, Twitter, Flickr or YouTube).⁶⁹

Finally, the law of 17 December 2021, which transposed the European Electronic Communications Code Directive (EEC Code Law), has expanded the definition of the term ‘electronic communication service’ compared to the one included in Article 2(k) of the 2005 Law on the Protection of Private Life and analysed before. More specifically, Article 2(4) of the EEC Code Law reads as follows:

‘electronic communications service’ means a service normally provided for remuneration via electronic networks, which encompasses, with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services, the following types of services:

- (a) ‘internet access service’ as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;
- (b) interpersonal communications service; and
- (c) services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting.

mai 2005 sur les réseaux et les services de communications électroniques (2005 Law on Electronic Communications Networks and Services), 30 May 2005, Mémorial A73, 7 June 2005, which had been the first law to move away from the old term ‘telecommunications’. The 2011 Law was subsequently repealed by the EEC Code law (for more details, see later in this section).

⁶³ Loi du 21 mars 1997 sur les télécommunications (Telecommunications Law), 21 March 1997, Mémorial A18, 27 March 1997.

⁶⁴ Telecommunications Law, Art. 2(26).

⁶⁵ Funck, ‘Luxembourg’, 191.

⁶⁶ 2005 Law on the Protection of Private Life, Art. 1.

⁶⁷ Ibid., Art. 2(k).

⁶⁸ A similar distinction between ECS and ISS was made by the Law of 27 February 2011 on Electronic Communications Networks and Services which was repealed by the 2021 EEC Code Law.

⁶⁹ Law on e-Commerce, Arts. 60–62.

It follows, therefore, that the EEC Code Law has brought some ‘over-the-top’ (OTT) service providers into the definition of ECS for regulatory purposes.⁷⁰ Such providers remain, however, exempted from any data retention obligation pursuant to Article 2(k) of the 2005 Law on the Protection of Private Life.

13.4 DOMESTIC COOPERATION BETWEEN LEAs AND SERVICE PROVIDERS

13.4.1 Introduction

Luxembourg LEAs tend to prefer cooperation with SPs based in Luxembourg or, at least, having some physical presence on the territory (e.g. data centres, offices, contact persons). The presence of the European headquarters of major service providers in the Grand Duchy even leads law enforcement to focus on those investigations which can draw on whatever data is accessible locally. The same can be observed regarding foreign SPs without an office in Luxembourg but keeping a copy of their data mirrored on local servers, obviating the need to resort to mutual legal assistance (MLA).⁷¹ While there is no formal obligation to keep data mirrored on local servers, some providers offering services in Luxembourg tend to follow this practice.

It is worth mentioning that the legislative framework for cooperation with SPs has been particularly focused on financial crime and especially anti-money laundering and the fight against terrorist financing. Furthermore, existing reports and research have suggested that cooperation within Luxembourg between judicial authorities and ISPs works fairly smoothly in practice – although the remit of the few (and now somewhat dated) available studies is limited to particularly grave offences: child sexual abuse online and the use of the internet for terrorist purposes.⁷² More recently, regarding cybercrime, a Council of Europe evaluation on Luxembourg’s capacities in that domain also found that local branches of private companies cooperate voluntarily with regard to subscriber information, and that overall cooperation is very good.⁷³ Companies do not, on the other hand, transmit information that they adjudge to have no link to Luxembourg. According to our exchanges with the Luxembourg police, the location of the data sought is usually deduced by using WHOIS.⁷⁴ Where this method is not available, the location of the headquarters of the internet service provider (ISP) is generally used as the location of the data. In response to our queries, the Ministry of Justice mentioned internet protocol (IP) address as the sole criterion for localising data, whilst a prosecutor merely stated

⁷⁰ Funck, ‘Luxembourg’, 185.

⁷¹ Braun, ‘La ratification de la Convention de Budapest’, 132. This conclusion is supported by voluntary transparency reports published by some Luxembourg-based ISPs. See, for instance, the Microsoft annual reports on law enforcement requests concerning Luxembourg, www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report.

⁷² See the aforementioned Microsoft annual reports on law enforcement requests concerning Luxembourg; Global Alliance against Child Sexual Abuse Online, 2014 Reporting Form for Luxembourg, stating that ‘the cooperation which is based on a non-written gentlemen [*sic*] agreement is excellent and works very well in practice’ (p. 2), https://ec.europa.eu/home-affairs/document/download/d50b9725-de0a-45dc-bd9d-c51cc1b8d1b2_en. See also Franssen and Ligeti, *The Cooperation of Service Providers with Judicial Authorities*, 20, with reference to the CODEXTER Report on the use of the internet for terrorist purposes in Luxembourg, October 2007: ‘There is no formal partnership between the public and private sectors, although the relevant police departments keep up excellent relations with the service providers and their co-operation is good on the whole.’

⁷³ More generally, see the first listed recommendation (of seven) made to the European Union, EU institutions and other member states in Council of the EU, Report on Luxembourg: ‘The Member States should take inspiration from the good practice identified by the evaluation team in Luxembourg, i.e.: – the excellent collaboration between the public sector and private sector’ (p. 100).

⁷⁴ The WHOIS database is a search service open to everyone that covers all domain names registered in the ‘.lu’ zone.

that the police investigation will determine where the data is stored. On an operational level, with the exception of basic subscriber information,⁷⁵ which is often provided without a judicial order, such an order is necessary for any other type of data sought. The length of time required to obtain the data sought depends on the availability of the LEAs to which the judicial authorities have recourse to enforce their orders.

In case of flagrancy – where an offence is in the course of being committed, has just been committed, or immediately after its commission the suspect is pursued or is found with items, traces or clues suggesting that the suspect participated in the commission of an offence – the police can proceed to coercive acts without prior authorisation of the investigating judge.⁷⁶ Such coercive acts include the seizure and access of data, and SPs can also be requested to assist. Given the lack of prior authorisation by an investigating judge, to safeguard the rights of the person concerned Luxembourg law provides for an *ex post* judicial review of preliminary investigations.

In general, the range of the duties incumbent on SPs encompasses retaining data, providing access to data and assisting the LEAs or the investigating judge or the public prosecutor in obtaining data by providing technical assistance and expertise. Before presenting in more detail the duties of SPs to cooperate with criminal investigations conducted by Luxembourg LEAs, it is worth highlighting a slight, recurrent disconnect between the scope of those duties on the one hand (some of which refer in several places to ‘telecommunications operators’) and the more recent regulatory terminology and data retention obligations on the other (which apply to ECS). An example is provided by ‘track and localise’ orders (discussed in more detail in Section 13.4.3). Although the distinction between the tracking of telecommunications data and the localisation of the origin and destination of telecommunications in the CCP is comparable to that found in the data retention provisions between traffic data and ‘location data other than traffic data’, the CCP provisions are limited to operators and providers of telecommunications services. Similarly, the new Chapter XII of the CCP, inserted by the 2018 Law on Terrorist Threats, refers to the ‘identification of a user of telecommunications’ and establishes the powers of the public prosecutor or investigating judge to require telecommunications operators or SPs to divulge certain subscriber and usage data.

13.4.2 Nature of the Cooperation

In Luxembourg there is a mix of mandatory and voluntary cooperation between SPs and the public authorities. However, there are no official statistics available that would reveal the relative weight of each investigative route in practice.

13.4.3 Overview of Existing Cooperation Duties

The cooperation of SPs with LEAs takes varied forms that cover not only data retention but also other duties, such as providing assistance to the LEAs in identifying subscribers/common users, tracking and localising suspects, getting access to an IT system, enabling the interception of data,

⁷⁵ Following the approach of the Cybercrime Convention Committee of the Council of Europe (T-CY), Luxembourg considers IP addresses as subscriber information when they refer to specific communications and irrespective of their fixed or dynamic character. See also Council of Europe, *T-CY Guidance Note #8: Obtaining Subscriber Information for an IP Address Used in a Specific Communication within a Criminal Investigation*, T-CY (2013) 26, 12 November 2013, pp. 4–5, <https://rm.coe.int/16802e7130>.

⁷⁶ CCP, Art. 48–26. See also V. Covolo, ‘Luxembourg’, in S. Allegrezza and V. Covolo (eds.), *Effective Defence Rights in Criminal Proceedings: A European and Comparative Study on Judicial Remedies* (Milan: CEDAM, 2018).

and decrypting data when the LEAs conduct investigative measures without the direct involvement of SPs.

The cooperation duties of SPs may be activated in the context of the following investigative measures:

- rapid preservation (quick freeze) of data (Article 48-25 CCP)
- production order (Articles 48-27 and 67-1 CCP);
- search of an IT system (Article 66 CCP);
- interception of data (Articles 88-1 to 88-4 CCP).

13.4.3.1 Data Retention and Rapid Preservation (Quick Freeze) of Data

Duties relating to data retention include the duty to retain data and to update the ILR central registry as discussed in detail at Section 13.2.2, as well as the rapid preservation or quick freeze of data. According to Article 48-25 CCP, inserted by the Law of 18 July 2014 which implemented the Budapest Convention, where there are grounds to believe that data stored, processed or transmitted by means of an IT system is particularly vulnerable to loss or modification, the public prosecutor or the investigating judge may order its ‘rapid and immediate’ preservation. Article 48-25 CCP seems to cover not only traffic data but any type of data including content data, and therefore it goes beyond the minimum threshold laid down by the Budapest Convention.⁷⁷ Rapid preservation can last for a maximum of ninety days. Although Article 48-25 CCP does not specify the addressee of a preservation order, it can be any person having the data in their possession or under their control, including SPs. This finds support in Article 16 of the Budapest Convention, which provides that

Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data *in the person’s possession or control*, the Party shall adopt such legislative and other measures as may be necessary *to oblige that person to preserve* and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure.⁷⁸

13.4.3.2 Production Orders

The most important form of cooperation is to comply with a production order, whether it concern content, traffic or location data, or identification/subscriber data. A duty to assist in unveiling traffic and location data is stipulated in Article 67-1 CCP. It is addressed to telecommunications operators or, more generally, SPs of telecommunication services and has the purpose of tracking and localising those suspected of criminal acts that may be punished with a maximum term of criminal or correctional imprisonment of at least one year.⁷⁹ Relying on the (older) assumption that traffic data is far less sensitive than content data, the decision of the investigating judge to authorise an Article 67-1 order need not take the form of a detailed decision but can merely indicate the factual circumstances of the case which justify recourse to such an

⁷⁷ Article 48-25 CCP applies to data that is ‘stored, processed or transmitted’ by means of an IT system, and it does not restrict its scope to traffic data.

⁷⁸ Cybercrime Convention, Art. 16(2) (emphasis added).

⁷⁹ A criminal imprisonment is a penalty that may be inflicted on those who commit crimes, whereas (less evidently) a correctional imprisonment is a penalty that may be inflicted on those who commit misdemeanours.

order. The SP must be informed of the duration of the measure, which must be specific and cannot exceed one month, subject to subsequent renewal with no ultimate maximum period foreseen.⁸⁰ Compliance is mandatory, and provided as soon as possible.⁸¹ Additionally, all persons involved in assisting with the investigation are under an obligation of secrecy. Refusal to assist with tracking and localising suspects is punishable with a fine of 100 euros to 5,000 euros.

Furthermore, the new Chapter XII of the CCP, inserted by the Law of 27 June 2018 on terrorist threats, requires SPs to divulge certain subscriber and usage data as defined in Article 10bis of the 2005 Law on the Protection of Private Life.⁸² This cooperation duty is addressed to telecommunications operators or, more generally, SPs of telecommunication services and has the purpose of identifying a subscriber or common user.⁸³ To gain access to this data, a written and reasoned order is required which should comply with the principles of proportionality and subsidiarity.

In certain urgent cases,⁸⁴ the judicial police officers may request this data upon the oral agreement of the public prosecutor or the investigating judge. The compliance of SPs is mandatory, and their assistance needs to be provided as soon as possible. The refusal of providing technical assistance is punishable with a fine of 1,250 euros to 125,000 euros.

13.4.3.3 Searches of an IT System

As mentioned in Section 13.2.1, the Law of 19 July 2014 implementing the Budapest Convention introduced procedures for the seizure of stored data – including content data – by the investigating judge in the course of a judicial inquiry or the public prosecutor in the limited *mini-instruction* scenario.⁸⁵ In the context of searches, Article 66 CCP sets another cooperation duty for SPs. The investigating judge can order any person that they deem to have special knowledge of the IT system, or of services that are used to secure or encrypt data, to provide access to a seized system, access to data contained within or accessible from such a system, or an understanding of data that is seized but protected or encrypted.

13.4.3.4 Interception of Data

Articles 88-1 to 88-4 CCP set out a series of special measures enabling the interception of all forms of communications, and all types of data, strictly by the investigating judge in the course of a judicial inquiry. These measures rely on the mandatory cooperation of SPs and cover the interception of telecommunications and postal correspondence and the capture of IT data.⁸⁶

⁸⁰ CCP, Art. 67-1(1).

⁸¹ CCP, Art. 67-1(2).

⁸² As amended by the Law on Terrorist Threats. For more details, see Section 13.2.2.

⁸³ CCP, Article 48-27. See also 2005 Law on the Protection of Private Life, Art. 10bis(4) as amended by Law of 27 June 2018.

⁸⁴ In the event of urgent need to prevent a serious attack on the life, freedom or physical integrity of a person or where it is imperative that the authorities competent for the investigation act immediately to avoid jeopardising serious criminal proceedings.

⁸⁵ CCP, Arts. 31 and 33. See further Ligeti and Robinson, ‘The Handling of Digital Evidence in Luxembourg’, 123–163.

⁸⁶ The interception of telecommunications is available only in relation to the prosecution of offences carrying a maximum sentence of at least two years’ imprisonment. The capture of IT data is limited, by contrast, to crimes and misdemeanours against state security, acts of terrorism and terrorist financing. See CCP, Art. 88-2(1)–(2), as amended by the Law on Terrorist Threats, Art. 1(6). The main changes in the 2018 reform are the following: a more flexible extension of twenty-four-hour detention; undercover online investigations (*enquête sous pseudonyme par voie électronique*); searches of premises at any time of day or night; placement of devices in private premises in order to carry out audio or visual surveillance.

Article 88-4 CCP provides that the SPs are notified of the decision of the investigating judge to intercept data and they proceed without delay to executing the measures. Under Article 88-4 CCP, the refusal to provide such assistance is punished with a fine of 1,250 euros to 125,000 euros. It is worth underlining that refusal to cooperate constitutes a criminal offence and the fine is thus a criminal penalty. In practice, SPs will only exceptionally receive an order from the judicial police (or directly from an investigating judge) to assist with such measures, and only after a detailed decision from the investigating judge.

Finally, Article 88-4 CCP provides an additional duty of assistance incumbent on SPs – similar to that in Article 66 CCP – regarding password- or encryption-protected data. The investigating judge can order any person other than the suspect to provide access to an IT system, access to data contained within or accessible from an IT system, as well as an understanding of data that is protected or encrypted (implying decryption of data).

13.4.4 *Legal Remedies and Protection of Fundamental Rights*

Before introducing available legal remedies in the context of the collection and use of personal data for investigatory purposes, it is worth giving a brief overview of the provisions on confidentiality/secrecy in Luxembourg law. The apex norm is Article 28 of the Luxembourg Constitution: the confidentiality of correspondence (*'secret des lettres'*) is inviolable. The same provision adds that the law determines the (postal) agents responsible for any violation of this principle, as well as the protections to be granted to communication by telegram. Despite not explicitly covering new technologies and electronic forms of communication, this provision illustrates that in Luxembourg confidentiality is guaranteed by constitutional provisions.

Additionally, several statutory provisions entrust SPs and operators with guaranteeing confidentiality and require the consent of the user for any interception, storage or monitoring. Such consent is usually given beforehand, with the approval of the terms and conditions. Specific provisions govern the retention of and access to data, according to the type of data and the purpose of retention or access.⁸⁷ Express derogations are also provided regarding interception of and access to data for cases of flagrant crime, the safeguarding of state security, defence and public safety, as well as the prevention, detection, establishment (*constatation*) and prosecution of criminal offences.⁸⁸ Infringement of the relevant safeguards on confidentiality can lead to imprisonment, to a fine and to a daily financial penalty in case of continued violations.⁸⁹ The second limb of Article 509-3 of the Criminal Code, as modified after the 2014 law implementing the Budapest Convention, provides for imprisonment of between three months and three years, as well as for a fine between 1,250 euros and 12,500 euros, for unauthorised and intentional data interference or interception. Those sanctions can be pronounced cumulatively.

Regarding more specifically legal remedies and respect of fundamental rights during investigatory measures, it is also important to stress the two-pillar architecture of judicial protection in Luxembourg. The first pillar relies on the suspect and on their capacity to bring a case before

⁸⁷ For instance: access to content and traffic data for the purpose of ensuring effective assistance in case of a call to the emergency number 112. Traffic data must be deleted once emergency assistance is provided; content (i.e. recordings of calls or voicemails, which may need to be 'listened back to' in case of misunderstandings or ambiguity between caller and responder) must be deleted after six months at the most. See 2005 Law on the Protection of Private Life, Art. 4(3)(c).

⁸⁸ Ibid., Art. 4(3)(b).

⁸⁹ Ibid., Art. 4(4).

a judicial organ. The second pillar relies on the investigating judge, whose orders must comply with specific obligations designed to facilitate judicial appraisal of the proportionality and necessity of investigative acts. The necessity of more-intrusive investigative measures, such as access to some types of data, needs to be justified by weighing the potential effectiveness of conventional investigation methods together with the exceptional nature of the case at hand. In that context, the interception and monitoring of telecommunications must always be duly justified relying on the factual background of the case.

While there is no specific procedure or remedy in Luxembourg to directly challenge acts of cooperation carried out by SPs, it is possible – in principle, for any party with a legitimate interest – to request the nullity of (an act of) a preliminary investigation or judicial inquiry, including investigative measures relating to the retention or processing of personal data.⁹⁰

A brief overview of the remedies available for different data categories that might be concerned by investigative measures can provide a more specific understanding of the legal protection offered under Luxembourg law. While the seizure of stored content data is amongst the most intrusive of investigative acts and thus requires due justification under penalty of nullity of the measures involved, the interception of content data sits within a similarly protective regime. In practice, challenging the validity of measures relating either to seizure or to interception of content data presents two difficulties. First, the data subject usually learns of the execution of such measures at the end of the preliminary investigation or judicial inquiry. Therefore, a long period of time is passing between the execution of the measure and the moment when the data subject is able to lodge a request for annulment of the measures. Second, the time limit to take action is only five days. According to Article 88-4(8) CCP, the seized or intercepted data is destroyed after a decision to acquit becomes final or after the prescription date. In case of conviction, the data is not destroyed. Concerning traffic and location data, legal remedies are available at an earlier time than those relating to content data. Indeed, for traffic and location data gathered via ‘track and localise’ orders, Article 67-1(3) provides that the data subject is informed during the investigation and no later than twelve months after the execution of the measure. The only exception to this rule concerns ‘track and localise’ orders regarding serious organised crime and terrorism. A similar regime to the *mini-instruction* is applicable.⁹¹ No specific safeguard is provided for access to or collection of subscriber data, despite the existence, since the 2018 Law on Terrorist Threats, of the ILR’s central registry of subscriber and usage data. The only legal remedy for this type of data would be available once a decision to proceed to trial is taken. At that stage, possible grounds for the annulment of such measures might be found in the requirements of Artobis of the 2005 Law on the Protection of Private Life: for instance, consultation of the registry must be by secured means, data consulted must be directly linked to the facts initially warranting access, and the time and duration of consultations must be recorded.

From a systemic perspective, the Luxembourg regime of all available legal remedies is characterised by a rather rigorous approach in terms of time limits and of the moment the data subject is effectively informed about measures taken regarding their data. This approach manifests the specific choices of the Luxembourg legislator regarding the balance to be struck between, on the one hand, private interest and fundamental rights and, on the other, the public interest in adequately equipped and effective law enforcement.

⁹⁰ CCP, Arts. 48-2 and 126.

⁹¹ CCP, Art. 24-1. For a brief description of the *mini-instruction*, see note 12.

13.5 CROSS-BORDER COOPERATION BETWEEN LEAs AND SERVICE PROVIDERS

13.5.1 *Introduction*

No exhaustive list of criteria is provided in Luxembourg law for defining the location of data and the cross-border nature of an investigation or direct data request. In practice, the cross-border nature of (direct) cooperation with SPs depends on the location of the headquarters of the SP holding the data or the location of the IP address of the persons subject to the investigation. Similarly, there is no specific provision regulating cross-border cooperation between LEAs and SPs. The cross-border cooperation of domestic LEAs with foreign SPs depends on the legal framework applicable in the state where the data is located, even when the CCP provides for the extraterritorial application of Luxembourg laws. The cross-border cooperation of foreign LEAs with SPs based in Luxembourg relies mainly on indirect cooperation, with the mediation of Luxembourg authorities. In that regard, it is worth mentioning that the quick freeze measure, available for the domestic cooperation of Luxembourg LEAs with Luxembourg-based SPs, also applies following the receipt of a request from a foreign competent authority.⁹² Additionally, the 2018 LED Law defines the term of ‘competent authority’ – for the purpose of the law at hand which sets rules on the protection of persons with regard to the processing of personal data in criminal proceedings – in a way that encompasses not only Luxembourg LEAs but also LEAs of other member states.⁹³ Based on such a definition,⁹⁴ one could think that direct cooperation between EU LEAs and Luxembourg-based SPs is possible under Luxembourg law; nevertheless, domestic law has not imposed this duty of cooperation on Luxembourg-based SPs.

In fact, the extent of direct cooperation of Luxembourg-based SPs and foreign (EU or third country) LEAs remains unclear as no transparent information is produced and publicly circulated.⁹⁵ There is also limited available information regarding indirect cross-border cooperation, and the numbers of incoming requests for MLA and EIOs remain low despite the presence in Luxembourg of the European headquarters of several significant SPs. This might be explained by the fact that the data is not necessarily stored at the physical place of the headquarters and that it might be more effective for foreign LEAs to request that data directly from other (non-European) branches of the relevant SP. Another plausible explanation is that indirect cooperation tools are principally used to access data that is not typically controlled by IT service providers, such as banking information.⁹⁶ At the same time, a prosecutor highlighted the types of offences in relation to which Luxembourg authorities receive requests for cross-border

⁹² *Projet de Loi n° 6541 portant: (1) approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001; (2) approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003; (3) modification du Code pénal; (4) modification du Code d'instruction criminelle; (5) modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques (Bill 6514), 8 January 2013, Commentaire des articles (Article-by-article commentary), p. 13.*

⁹³ See especially LED Law, Arts. 1(1) and 2(7)(b).

⁹⁴ Pursuant to Article 2(7)(b) of the LED Law, a ‘competent authority’ can be ‘any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security’.

⁹⁵ Representatives from Amazon declined to officially participate in an interview with our research team.

⁹⁶ According to the representative of a law firm, the majority of requests received by the Luxembourg judicial authorities are indeed related to this type of banking data and are emanating from neighbouring countries such as France, Belgium, Italy, the Netherlands and Switzerland.

access to data: fraud (*escroquerie*), IT offences, theft, and possession of child pornography images.⁹⁷ A contact at the police has even stressed that, in terms of numbers of requests, cybercrime and financial crime come first. Even if those characteristics of indirect cooperation might suggest that some type of data is obtained via direct channels of cooperation, no formal evidence can confirm it.

13.5.2 Cooperation of National LEAs with Foreign Service Providers

Although no official statistics exist, a police source cited organised crime, cybercrime and financial crime as the main types of investigations leading to Luxembourg-origin requests for indirect or direct cooperation, whilst a view from academia mentioned child pornography, financial crime and hacking. Cooperation between Luxembourg law enforcement and foreign SPs appears to be rather challenging, although detailed statistics here too are still scarce. According to an investigating judge, in 2021 LEAs issued 301 EIOs and 31 letters rogatory addressed to EU and third-country national authorities respectively requesting data kept by SPs established abroad, while the number of direct requests to foreign SPs is unknown.⁹⁸

Cross-border voluntary cooperation would appear to be much easier for less-sensitive data: a contact at the Ministry of Justice stated that ‘more intrusive data, such as content or transactional data’, are in practice subject to stricter controls (by foreign SPs in case of direct cooperation or by foreign authorities in case of indirect cooperation) in order to ensure respect for fundamental rights. According to an investigating judge, only some SPs are willing to cooperate directly with the LEAs voluntarily; and those providers usually hand over only basic subscriber information.⁹⁹ Even where foreign SPs cooperate voluntarily, they may not transmit information that they adjudge to have no link to Luxembourg. In such cases, in order to access subscriber information and, especially, content data, the police must ask an investigating judge to issue letters rogatory, considerably slowing down the process.¹⁰⁰ By contrast, cooperation with local SPs is smoother. A specialised public prosecutor observed that ‘cooperation with service providers other than providers hosting information provided by a recipient of the service is quite good in practice, especially if those providers have their headquarters, an office or at least a contact point in Luxembourg’.¹⁰¹

From our exchanges with an investigating judge, it would appear difficult in many cases to obtain electronic data from certain third countries, whilst in the course of a 2017 GENVAL Evaluation of Luxembourg’s response to cybercrime, practitioners indicated that large US-based ISPs ‘often refuse to communicate data concerning offences related to the incitement of hatred, retreating behind freedom of expression’.¹⁰²

13.5.2.1 Legal Framework

Direct cooperation between Luxembourg LEAs and foreign SPs is not provided for by law. It can, however, be decided to seek such cooperation in light of the factual context of an investigation. In this case, the cooperation would be either merely voluntary or bound by the

⁹⁷ In the same vein, see also Council of the EU, Report on Luxembourg, 85.

⁹⁸ Interview with a Luxembourg investigating judge. According to the same source, in 2020 LEAs issued 312 EIOs and 35 letters rogatory.

⁹⁹ Interview with a Luxembourg investigating judge. On this topic, see more at Section 13.5.2.2.

¹⁰⁰ Council of the EU, Report on Luxembourg, 90.

¹⁰¹ This information results from an interview conducted at the University of Luxembourg in 2014. An investigating judge has also confirmed this understanding. See Interview with a Luxembourg investigating judge.

¹⁰² Council of the EU, Report on Luxembourg, 90.

laws of the country hosting the SP holding the data. From the perspective of the Luxembourg LEAs, it is necessary to abide by the applicable laws in Luxembourg regarding data protection as well as coercive investigative measures. In other terms, in case of direct cooperation with foreign SPs, and despite the lack of a specific legal framework, the principles applicable to domestic cooperation should be observed in order to avoid the risk of nullity of the investigative act and inadmissibility of the gathered evidence. A crucial element in engaging in direct cooperation with foreign SPs lies in the role of the investigating judge. Indeed, by virtue of Article 51 CCP, the search for the truth conducted by the investigating judge should examine ‘with equal care’ the facts and circumstances tending to incriminate or exculpate (*à charge ou à décharge*). As part of the investigation, the request for direct cooperation should be aligned with this principle.

On the other end of the spectrum, the indirect cooperation of Luxembourg LEAs with foreign SPs relies either on MLA, in the case of non-EU countries, or on the EIO, in the case of EU member states.¹⁰³ Luxembourg implemented Directive 2014/41/EU on the European Investigation Order in September 2018.¹⁰⁴ Before the entry into force of the implementing law, cooperation requested by the Luxembourg authorities (*entraide active*) was the subject of no dedicated framework in national law. By contrast, the MLA Law¹⁰⁵ provided the foundation in national law for so-called *entraide passive*, meaning cooperation provided to foreign judicial actors by their Luxembourg counterparts, including in relation to accessing electronic evidence. Within the EU Area of Freedom, Security and Justice, from September 2018 onwards the EIO implementation law replaced the MLA Law along with the national corresponding provisions of the main multilateral MLA Conventions and Treaties¹⁰⁶ as concerns all relations between Luxembourg and other EU member states having also implemented the EIO Directive vis-à-vis cross-border access to electronic data in the context of criminal investigations and proceedings.¹⁰⁷ Nevertheless,

¹⁰³ Ireland and Denmark have negotiated general opt-outs regarding the Area of Freedom Security and Justice. In this regard, see Protocol No. 21 on the Position of the United Kingdom and Ireland in Respect of the Area of Freedom, Security and Justice, [2016] OJ C 202/295, 7 June 2016, and Protocol No. 22 on the Position of Denmark, [2012] OJ C 326/299, 26 October 2012. For a specific analysis of this point, see S. Tosza, ‘All Evidence Is Equal, but Electronic Evidence Is More Equal Than Any Other: The Relationship between the European Investigation Order and the European Production Order’ (2020) 11(2) *New Journal of European Criminal Law* 161–183.

¹⁰⁴ EIO Law.

¹⁰⁵ Loi du 8 août 2000 sur l’entraide judiciaire internationale en matière pénale (MLA Law), 8 August 2000, Mémorial A98, 18 September 2000, as amended by the Loi du 27 octobre 2010 portant 1. approbation de la Convention du 29 mai 2000 relative à l’entraide judiciaire en matière pénale entre les États membres de l’Union européenne, 2. approbation du Protocole du 16 octobre 2001 à la Convention relative à l’entraide judiciaire en matière pénale entre les États membres de l’Union européenne, 3. modification de certaines dispositions du Code d’instruction criminelle et de la loi du 8 août 2000 sur l’entraide judiciaire international en matière pénale (Law Implementing the EU MLA Convention), 27 October 2010, Mémorial A194, 3 November 2010.

¹⁰⁶ Council of Europe, European Convention on Mutual Assistance in Criminal Matters, ETS No. 30, 20 April 1959 and its additional protocols; Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, 19 June 1990, OJ L 239, 22 September 2000; Council of the European Union, Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, [2000] OJ C 197, 12 July 2000; and Secrétariat Général Benelux, Traité Benelux d’extradition et d’entraide judiciaire en matière pénale avec Protocole concernant la responsabilité civile pour les agents en mission sur le territoire d’une autre Partie, signés à Bruxelles, le 27 juin 1962 (1962 Benelux Treaty on Extradition and Mutual Assistance in Criminal Matters), Bulletin Benelux 1967-7, p. 1.

¹⁰⁷ EIO Law, Art. 42(1). Moreover, the new law also stipulates that requests for assistance originating from ‘States’ – meaning, presumably, EU member states – which have *not* implemented the EIO Directive shall be ‘assimilated’ to requests made on the basis of the provisions of the EIO Directive and examined in accordance with the provisions of the implementing law. See EIO Law, Art. 42(2).

it should be noted that the 2018 law did not fundamentally change the nature of cooperation between SPs and Luxembourg LEAs, as will be demonstrated in Section 13.5.2.2.¹⁰⁸

Finally, in the context of the Council of Europe, a second Additional Protocol to the Budapest Convention was recently adopted, inter alia, establishing a legal basis for direct cooperation with foreign SPs for subscriber information and enhanced cooperation tools for the disclosure of subscriber information and traffic data.¹⁰⁹ Luxembourg was amongst the first parties to sign the Protocol on 12 May 2022, but has not yet ratified it.

13.5.2.2 Nature of the Cooperation

As explained in Section 13.5.2.1, Luxembourg LEAs cooperate with foreign SPs either directly on a voluntary basis or indirectly relying on traditional MLA requests or EIOs, depending on whether the SP is established in a third country or a member state of the EU. It appears from our exchanges with an investigating judge that some SPs, such as Facebook and Google, respond voluntarily to direct requests from Luxembourg LEAs.¹¹⁰ In the case of Facebook, direct requests from Luxembourg LEAs – and more broadly EU authorities – for basic subscriber information (e.g. name, email address, date of birth, telephone number and registration IP address) should be addressed to ‘Meta Platforms Ireland Ltd’. By contrast, traffic and content data may only be disclosed upon an MLA request to the US authorities. Google also cooperates directly with EU authorities when the requests are submitted to ‘Google Ireland Ltd’. Information that Google may disclose in the context of voluntary cooperation may include information related to the registration of the account (e.g. name, telephone number, email address), timestamps, recent IP addresses, Android subscriber information (e.g. device serial number, Android ID number, Gmail accounts logged into on the device and network connections). Therefore, the scope of direct voluntary cooperation is mostly limited to non-content data.

As noted earlier, there are also foreign SPs who are not willing to cooperate directly with Luxembourg LEAs. In these cases, the requests for cooperation should be addressed to the competent national authorities by way of an EIO or MLA request.

Where bilateral agreements with third countries are in place, the prosecutor or the investigating judge is empowered by such arrangements to make requests directly to counterparts, according to the terms of the base agreement.¹¹¹ Should there be no bilateral agreement, Luxembourg law still provides no general legal framework for the cooperation of Luxembourg LEAs with foreign authorities, which ‘is more a question of good sense than of law’.¹¹² Moreover, the possibilities for Luxembourg judicial actors to address letters rogatory or requests for MLA to the authorities of other countries already emerged from the very roles and powers of the assorted actors (principally, the public prosecutor and the investigating judges) in the domestic context as set out in the CCP, coupled with the numerous international conventions providing for letters

¹⁰⁸ Interview with a Luxembourg investigating judge.

¹⁰⁹ Council of Europe, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CETS No. 224, 27 November 2021.

¹¹⁰ Interview with a Luxembourg investigating judge.

¹¹¹ It is worth recalling here that the investigating judge requires the indictment (*réquisitoire*) of the public prosecutor in order to ‘inform’ (i.e. open) a judicial inquiry.

¹¹² See F. Lugentz, J. Rayroud and M. Turk, *L’entraide pénale internationale en Suisse, en Belgique et au Grand-Duché du Luxembourg* (Brussels: Larcier, 2014), 754 *et seq.*, who list as principal factors in any decision to request MLA (1) the usefulness of the act requested, (2) the proportionality of the means envisaged, (3) the probability of obtaining a result and, in keeping with Article 6 of the European Convention on Human Rights, (4) the length of time likely required in order to obtain the solicited material – especially in cases of preventive detention.

rogatory or MLA requests which Luxembourg has ratified and which – owing to the monist tradition of Luxembourg vis-à-vis international law – sit within the national legal order.

Whichever route is taken, practitioners in Luxembourg have expressed dissatisfaction with both the EIO and the MLA system in respect of the collection of electronic evidence. In terms of the time frame, a source at the Ministry of Justice estimated that it takes on average 120 days to receive electronic data requested from an EU member state,¹¹³ and up to 300 days where it is requested from a third state (e.g. the US).¹¹⁴ Where data is stored in another country, noted a prosecutor, international requests for cross-border access take longer since they depend on the workload and willingness to assist of the receiving judicial authority. A source at the Ministry of Justice cited verification of the validity and legality of requests, the volume of data requested and encryption of data as the main challenges in this regard, whilst a view from the police emphasised that ‘the knowledge of what information is available where and how might take time to acquire’; thereafter, letters rogatory must be drafted – but ‘most of the time’ is taken up by waiting for a reply. According to one legal professional close to the Luxembourg LEAs, the slow handling of requests emitted by Luxembourg can be ascribed to the lack of willingness of receiving authorities, along with a lack of dynamism on the part of the Luxembourg authorities, who are not very ‘aggressive’ in chasing up requests. Transposed to the context of direct cooperation with foreign SPs, the same pattern suggests that such cooperation proves to be not only time-consuming but also rather ineffective. Developing a more demanding approach in terms of following up requests of direct as well as indirect cooperation might thus be an important action point for Luxembourg LEAs.

13.5.2.3 Legal Remedies and Protection of Fundamental Rights

Direct cooperation between Luxembourg LEAs and foreign SPs can only be challenged indirectly when attacking specific investigative acts. The same principles and procedures mentioned in Section 13.4.4 are applicable. As for judicial control of indirect cooperation between Luxembourg LEAs and foreign SPs, it should be noted that, despite the existence of safeguards, the legal remedies available are also directed against investigative acts (and not the act of cooperation as such).

In the presence of specific international agreements for MLA, or in the context of the EIO, the general domestic regime of data protection as well as the overarching rules of the CCP are to be observed by the Luxembourg LEAs and thus form a shield for data subjects. Even in the absence of an international agreement providing for the terms of the indirect cooperation, the Luxembourg authorities must of course refrain from requesting the execution abroad of measures which would be incompatible with the CCP – or risk seeing the request for cooperation, along with the subsequent acts, annulled.¹¹⁵

¹¹³ While those numbers refer to both traditional cooperation and use of the EIO, it needs to be noted that since the introduction of the EIO the time frame has been reduced. See, for instance, *Statistiques des juridictions et des parquets*, 2021, <https://justice.public.lu/dam-assets/fr/publications/rapport-activites-judiciaires/rapport-dactivite-2021-jj-version-web.pdf>.

¹¹⁴ Those numbers concern all requests, irrespective of the type of data sought.

¹¹⁵ The result of the annulment would be that the collected evidence becomes inadmissible before Luxembourg courts. See also Lugentz, Rayroud and Turk, ‘L’entraide pénale’, 733, where the authors, writing on the former Code d’instruction criminelle (now the CCP), considered the alignment with the national Code of cross-border cooperation requested by the Luxembourg Prosecutors or Instruction Cabinets to constitute an exception to the principle *locus regit actum* – since the target of an investigation may benefit from procedural safeguards enshrined in Luxembourg law, whichever state executes the measure.

As an act forming part of the investigation, the decision taken in Luxembourg by either the public prosecutor or an investigating judge to issue letters rogatory or an MLA request to colleagues abroad is in principle open to challenge according to the provisions of the CCP. A request for cooperation that does not lead to coercive measures towards the data subject, issued by a prosecutor or an investigative judge, may be challenged by any person able to show a personal interest in the matter before the pre-trial chamber. An interested person has two months from the emission of the request for cooperation to lodge the action for annulment, irrespective of whether the police investigation has or has not been followed by a judicial inquiry. However, where a judicial inquiry has been opened on the basis of the same police investigation, the accused has five days to lodge the action. The pre-trial chamber addresses the matter urgently and where it finds cause it annuls the act.¹¹⁶

A request for cooperation that leads to coercive measures regarding the data subject (especially when sensitive data is concerned), issued by an investigating judge, may be challenged by the chief public prosecutor, the accused as well as any plaintiff or third party with a personal interest in the matter before the pre-trial chamber. The action must be lodged within five days of being made aware of the challenged act. Differently to challenges to acts executing in Luxembourg, in relation to requests for cooperation from a foreign LEA (which are not public and – since 2010 – in relation to which the applicant may merely contribute observations on the regularity of the procedure), debates before the pre-trial chamber concerning the potential annulment of the request for cooperation posited by the Luxembourg judicial actors take place in the presence of interested parties, who are invited to attend.¹¹⁷ Lastly, the same regime is applicable in relation to the judicial control of EIOs issued by Luxembourg.

Crucially, however, since the concrete investigative measures requested by the judicial actors in Luxembourg are eventually executed in the other jurisdiction involved (thereby escaping national judicial control), litigation concerning the initial MLA request or EIO issued in Luxembourg is reported to be rare, in contrast – historically – to challenges to cooperation initiated by foreign LEAs, whereby investigative measures are executed in Luxembourg.¹¹⁸

13.5.3 *Cooperation of National Service Providers with Foreign LEAs*

As noted in Section 13.5.2.1, Luxembourg law does not provide any rules regarding the direct cooperation of domestic SPs with foreign LEAs. In principle, the cooperation between those actors is indirect, through the Luxembourg competent authorities and via the relevant instruments of indirect cooperation (MLA, EIO). While the Budapest Convention allows direct cooperation of foreign LEAs with domestic SPs that offer services in the country of the LEA concerned with seeking subscriber data,¹¹⁹ Luxembourg law remains silent on that matter as well as regarding any other type of data.

Thus, when foreign LEAs seek direct cooperation with Luxembourg-based SPs, the position of the latter can be difficult since they need to abide by the rules of the country where they have their headquarters (in this case Luxembourg) but also by the rules of the country where they provide their service, which is liable to contribute to the progress of a criminal investigation (by foreign LEAs). In the absence of clear rules in Luxembourg regarding the direct cooperation of domestic SPs with foreign LEAs, providing such assistance risks being deemed a violation of the

¹¹⁶ CCP, Art. 48-2.

¹¹⁷ CCP, Art. 126.

¹¹⁸ Lugentz, Rayroud and Turk, 'L'entraide pénale', 766.

¹¹⁹ Cybercrime Convention, Art. 18-1.

privacy and data protection obligations incumbent on the SPs by virtue of Luxembourg and EU law. The absence of a clear legal regime could thus lead to a de facto bar, or at least to the discouraging, of direct cooperation. This situation is particularly challenging regarding the LEAs of fellow EU member states as the very logic of the internal market (which applies also in those circumstances, especially regarding the commercial activities of the SPs),¹²⁰ of the Area of Freedom Security and Justice (which relies on mutual trust), but also of the common rules on privacy and data protection is not restrained by national boundaries.

In the absence of clear rules on the matter, the ‘Skype saga’ illustrates some of the current challenges regarding direct cooperation of Luxembourg-based SPs with foreign LEAs and introduces some suggestions.¹²¹ In 2012, a Belgian investigating judge issued a request for traffic data related to a suspected member of a criminal organisation directly to the Luxembourg offices of Skype. Skype refused to cooperate, offering to merely provide, on a voluntary basis, some subscriber information. According to Skype, traffic and location data as well as technical assistance to intercept communications could only be provided to LEAs of a state in which the company has no physical presence through indirect cooperation with its local (Luxembourg) authorities.¹²² While this interpretation of Luxembourg law is persuasive, it relies on the assumption that all European data subjects are beneficiaries of rights stemming from Luxembourg law, even if their sole link with Luxembourg is the fact that Skype has its European headquarters and some of its data centres on that territory. The key for the legal appraisal of this argument is whether all Skype clients, as data subjects, are indeed beneficiaries of rights stemming from Luxembourg law. This aspect is equally important to the argument advanced by the Belgian authorities and ultimately the courts, which did not hold indirect cooperation with Luxembourg to be necessary, and which in substance concluded that Belgian law was the sole applicable law since the data subjects under investigation were within the Belgian territory and Skype was offering services specifically addressed to the Belgian market. Neither law nor established practice allows us to favour one or the other of these two diametrically opposed interpretations. However, we believe that an important distinction is to be drawn between, on the one hand, situations of cooperation of Luxembourg-based SPs with EU LEAs and, on the other, of Luxembourg-based SPs with non-EU LEAs.

Indeed, while the application of legal safeguards and specific rights stemming from Luxembourg law to all data subjects receiving services from a Luxembourg-based SP, such as Skype, is not a far-fetched interpretation of Luxembourg law and could ground a refusal to cooperate directly with foreign LEAs, it cannot be overlooked that, on the one hand, principles governing privacy and data protection are common within the EU whilst, on the other, the action of EU LEAs is presumed to be compliant with EU law by virtue of the principle of mutual trust. In this context, the lack of specific national provisions allowing or prohibiting the direct cooperation of Luxembourg-based SPs with foreign (but EU) LEAs could not be the sole reason for declining direct cooperation. The lack of legal certainty is regrettable, yet the specific characteristics of the Area of Freedom, Security and Justice seem to support this kind of direct cooperation. The situation is significantly different when Luxembourg-based SPs are to

¹²⁰ Putting SPs established in Luxembourg (but exercising their activities also in the other member states) under contradictory, or at least unclear, duties can indeed hinder their freedom to provide services in the sense that they might face unpredictable pecuniary or other consequences in the different member states.

¹²¹ For a summary of the proceedings and critical commentary of the final Belgian judgment, see V. Franssen and M. Corhay, ‘La fin de la saga Skype: les fournisseurs de services étrangers obligés de collaborer avec la justice belge en dépit des possibilités techniques et de leurs obligations en droit étranger, Note sous Cass. 19 février 2019’ (2019) 8 *Revue de Droit Commercial Belge* 1014.

¹²² See also *ibid.*

cooperate with non-EU LEAs, where the applicable privacy and data protection regime is not founded on commensurate principles, and where the principle of mutual trust is not applicable to allow a presumption of conformity with some fundamental legal guarantees.

This context stresses the importance of regulating the direct cooperation of LEAs with SPs to go beyond the uncertain character of any voluntary cooperation. It also underlines the lack of a consensual criterion on the basis of which the duties applicable to SPs as well as the rules applicable to individual requests can be identified. While the Skype case is only a symptom of the lack of clear rules applicable beyond national boundaries, we posit that the lesson to be drawn does translate to a need to adjust Luxembourg law – or, rather, to do so without the equivalent adjustments being made in parallel in like-minded jurisdictions. Given that electronic communications are intrinsically globalised, it has been clear for some time that the solution should be more global, at least at the EU level. As we briefly unpack in Section 13.5.4, the recently adopted e-Evidence Regulation might thus become key in resolving the direct cooperation conundrum within the EU.

13.5.4 *Opportunities and Challenges Created by the Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Proceedings*

On 25 January 2023, the Council and the European Parliament reached an agreement on the draft regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Proceedings (e-Evidence Regulation).¹²³ The Regulation aims to introduce an alternative mechanism to the existing EU and international tools consisting in direct cooperation between national authorities and foreign SPs. More specifically, it enables national authorities to issue production and preservation orders directly to SPs based abroad in order to obtain or preserve e-evidence. Should SPs not comply with such orders, they may face penalties. Whilst the Regulation covers any category of data including subscriber, traffic and content data, some further limitations have been set in relation to traffic and content data. First, these can only be requested for crimes punishable in the issuing country by a maximum custodial sentence of at least three years, or for specific offences relating to cybercrime, child pornography, counterfeiting of non-cash means of payment or terrorism. Second, the issuing national authorities should notify the enforcing member state of the order so that the latter can raise one or more of the grounds for refusal laid down in the Regulation.

The e-Evidence Regulation is expected to overcome the shortcomings of the almost fifteen-year-old European Evidence Warrant that failed to become a workable instrument for cross-border cooperation on the collection of electronic evidence.¹²⁴ The very definition of the concept of electronic evidence by the e-Evidence Regulation appears at odds with the general logic of Luxembourg law, which does not rely on any particular distinction among categories of evidence. However, the Regulation is expected to bring clarity concerning the applicable rules on the direct cooperation of Luxembourg LEAs with SPs based in other EU member states, as well as of Luxembourg-based SPs with LEAs of other member states. Most of the uncertainties stemming from the voluntary nature of public–private cooperation for investigative purposes in

¹²³ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L191, 28 July 2023.

¹²⁴ On this topic, see also K. Ligeti and G. Robinson, ‘Sword, Shield and Cloud: Toward a European System of Public-Private Orders for Electronic Evidence in Criminal Matters?’, in V. Mitsilegas and N. Vavoula (eds.), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (Oxford: Hart, 2021), 27–70.

criminal proceedings should thus be lifted and a rather standardised form of public–private cooperation across the EU could be introduced.¹²⁵

The concrete way forward will require a delicate coordination between, on the one hand, the procedures and duties incumbent on SPs by virtue of the Regulation and, on the other, the existing national rules that affect those duties and even the sanctions resulting from non-compliance. The very need for coordination presents an additional challenge, especially given that duties and concepts used in Luxembourg law are linked to technical regulations concerning telecommunications, e-commerce or, more generally, data protection and retention rules. The flexible and pragmatic approach of Luxembourg in extending the use of sectoral duties and concepts to cover a variety of SPs¹²⁶ suggests that the challenge of coordination between the duties stemming from the e-Evidence Regulation and national provisions could, at least at a first stage, avoid any significant reform. However, the clarity of the legal framework applicable to this type of public–private cooperation can enhance (or, on the opposite, discourage) the effective cooperation of Luxembourg-based SPs and, ultimately, foster (or hamper) the practical success of the e-Evidence Regulation.¹²⁷

One specific point of Luxembourg law that will require clarification concerns the role of the CNPD in ensuring the observance of data protection obligations applicable to Luxembourg-based SPs, especially in cases of violation of rights.¹²⁸ As illustrated in the Skype case, SPs could indeed refrain from direct cooperation with LEAs from other member states to avoid a potential violation of Luxembourg rules. The obligation on the issuing LEA to inform its counterpart in the member state of the SP (in this case Luxembourg) about the data order addressed to an SP located (or legally represented) in this member state does not change the situation. An immediate change to the current Luxembourg regime, which dissuades direct cooperation, could stem from the enforcement procedure envisaged in the e-Evidence Regulation in case of refusal of a Luxembourg SP to execute an order issued by the LEA of another member state on grounds set out in Article 10(5) of the e-Evidence Regulation, such as potential interference with immunities or privileges. In such a scenario, where the issuing authority nonetheless wishes to maintain the order, it may be open to Luxembourg LEAs to waive the immunity or privilege,¹²⁹ before stepping in to enforce the data order, overriding the initial refusal of the Luxembourg-based SP following the procedure laid down in Article 16 of the e-Evidence Regulation.¹³⁰

The data categories that have finally been retained for the e-Evidence Regulation should not raise any specific problem of compatibility with the data classification in Luxembourg law. The main distinctions between content and non-content data, as well as the less stringent rules regarding subscriber data, secure a smooth continuation. The definition of the various data categories in the Regulation also facilitates a common approach from both SPs and LEAs regarding the requested data under the upcoming e-Evidence Regulation.

¹²⁵ See also *ibid.*, 29.

¹²⁶ This approach is illustrated by the extension of duties initially addressed to traditional telecommunication providers to cover also SPs that offer electronic forms of communication.

¹²⁷ One potential concern relates to the scope of application of sectoral duties and the more general scope of the upcoming e-evidence regulation. On this point, see also Ligeti and Robinson, ‘Sword, Shield and Cloud’, 30.

¹²⁸ On the role of the CNPD for ensuring the observance of data protection, see *Loi du 28 juillet 2011 portant modification (1) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques; (2) de la loi codifiée du 2 août 2002 relative à la protection des personnes à l’égard du traitement des données à caractère personnel; (3) de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l’Etat; (4) du Code de la consommation (2011 Data Protection Reform Law)*, 28 July 2011, *Mémorial A172*, 10 August 2011.

¹²⁹ e-Evidence Regulation, Art. 12(5).

¹³⁰ e-Evidence Regulation, Art. 16. See also Ligeti and Robinson, ‘Sword, Shield and Cloud’, 42.

13.6 CONCLUSION

This chapter's overview of the different aspects of cooperation between domestic or foreign SPs with domestic or foreign LEAs under Luxembourg law suggests that the latter is mainly focused on domestic situations and that its adaptation to the fast-changing context of data protection and of globalised electronic communications has been rather slow. While this is also true for all the member states of the EU, especially because of the restrictive case law of the CJEU regarding existing duties of SPs contributing to the fight against serious crime, it is necessary that Luxembourg assumes a proactive role in the regulation of the cooperation between SPs and LEAs. As the host of several major SPs, Luxembourg enjoys a central position for direct or indirect cooperation between those SPs and domestic or foreign LEAs. Nevertheless, Luxembourg law does not respond to the global challenges that are raised by the cross-border cooperation of SPs with LEAs. This observation stands not only regarding the non-existence of specific rules on the direct cooperation of domestic LEAs with foreign SPs but especially regarding the lack of rules on the direct cooperation of foreign LEAs with Luxembourg-based SPs. The ultimate source of such challenges lies of course in the absence of internationally approved criteria for the localisation of data and subsequently of the rules applicable to the SPs that hold them. However, the absence of Luxembourg laws on the direct cooperation of domestic SPs with foreign LEAs further deepens the legal uncertainty weighing on Luxembourg-based SPs and, as a result, sends contradictory messages as to the readiness of Luxembourg to be a main actor in the globalised context of SPs.

The rather introspective approach of Luxembourg law might be justified at the broader international level because it avoids sovereignty clashes and indirectly provides for safeguards regarding the data subjects linked to Luxembourg, but it proves to be untenable within the EU. This is especially so since privacy and data protection form important fields of EU law that are also related to the fundamental rights and principles of that legal order and could not legitimately give rise to mutual distrust among member states. Indeed, direct cooperation between EU LEAs and Luxembourg-based SPs constitutes a natural characteristic of an Area of Freedom, Security and Justice without internal boundaries and where the general principle of mutual trust leads to a (rebuttable) presumption that the investigative acts of other member states follow the fundamental principles and rights enshrined in EU law.

Undeniably, overcoming those challenges, which are common to all EU member states and not specific to Luxembourg, requires common action at the EU level. It remains to be seen, therefore, whether and to what extent the e-Evidence Regulation, which is being designed to enable direct cooperation between EU-based SPs and national authorities, will bring added value. However, benefiting from its position as a main host of international SPs, Luxembourg should envisage specific measures at this level, to contribute to the emergence of common principles and standards on the cooperation of EU-based SPs with EU LEAs. Such a proactive stance not only will enhance the clarity of the Luxembourg regime on the various aspects of the cooperation between LEAs and SPs but, most importantly, will contribute to the emergence of principles and standards fit to respond to global demands beyond the mere territorial limits of the EU.

Gathering of Digital Evidence and Cooperation of Service Providers in Poland

Maciej Rogalski

14.1 INTRODUCTION: SETTING THE SCENE

14.1.1 *General Approach to the Collection of Digital Evidence*

Under Polish law, the issue of the collection of digital evidence is regulated in a series of legal acts (statutes) and in regulations implementing those acts. Those regulations are not always coherent, which results in some interpretation problems. Moreover, the regulations are not updated often or quickly enough to keep up with technological changes. There is a lack of definitions of the concepts used in this area, especially concerning the concept of ‘electronic evidence’. Neither the Code of Criminal Procedure (CCP)¹ nor the Criminal Code (CC)² provides a definition of the term ‘electronic evidence’. This concept is used only by academics and in practice.

In the legal doctrine, the term ‘electronic evidence’ is used to refer to various types of evidence, in particular data seized in information systems or generated in the context of an interception of correspondence, wiretapping, information recorded on data carriers and so on.³ In practice, in criminal proceedings these types of evidence are analysed and assessed separately, according to the provisions applicable to each type. There are no provisions laid down in a single chapter that determine the criminal procedure that should apply to each type of electronic evidence. The provisions concerning electronic evidence are dispersed throughout the whole CCP, in each case dealing with only one issue.

A first provision on the gathering of electronic evidence is Article 218 § 1 CCP:

Offices, institutions and entities operating in post and telecommunications fields, tax and customs offices, and transportation institutions and companies shall be obliged to provide a court or a prosecutor with correspondence, post and data listed in a decision in accordance with Article 180c and Article 180d of the Telecommunications Law Act of 16 July 2004 (TL)⁴ if they are significant to the pending proceeding.⁵

¹ The Code of Criminal Procedure Act of 6 June 1997 (*kodeks postępowania karnego*), consolidated text, Journal of Laws (*Dziennik Ustaw*) of 2021, item 534, as amended (the ‘Journal of Laws’ is called ‘Dziennik Ustaw’ in Poland).

² The Criminal Code Act of 6 June 1997 (*kodeks karny*), consolidated text, Journal of Laws of 2021, item 2345, as amended.

³ A. Lach, *Dowody elektroniczne w procesie karnym* (Toruń: Dom Organizatora, 2004), 29–67; A. Adamski, *Prawo karne komputerowe* (Warsaw: C. H. Beck, 2000), 192 *et seq.*; E. Cassey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Baltimore, MD: Academic Press, 2000), 93 *et seq.*; P. Lambert, ‘The Search for Elusive Electrons: Getting a Sense of Electronic Evidence’ (2001) 1 *Judicial Studies Institute Journal* 24–27.

⁴ Telecommunications Law Act of 16 July 2004 (*prawo telekomunikacyjne*), consolidated text, Journal of Laws of 2021, item 576, as amended.

⁵ The translations of acts of law given here are not official translations, but were made by the author of this chapter.

Thus, the CCP does not regulate the aforementioned issue fully, but refers to the TL. This is also true in the case of the use of electronic evidence, but here the CCP refers not to the TL but to other provisions in other chapters of the CCP. For example, Article 236a CCP states that the provisions of Chapter 25 CCP concerning the seizure of objects and searches ‘are by analogy applicable to the holder or user of the devices containing information or the information system within the scope of data retained in the device or system or a data carrier at their disposal or in their use, including electronic correspondence’. Similarly, the provisions on the interception and recording of conversations (Articles 237 and following CCP) are applied analogously. In accordance with Article 241 CCP, ‘the provisions of this Chapter shall apply respectively to the interception and recording of the content of other conversations or information transmissions with the use of technical means, including electronic correspondence’.

The above provisions of the TL concern telecommunications data as defined in Articles 180c and 180d TL. Additionally, the Act on the Provision of Electronic Services (ESA)⁶ provides for the possibility to collect data as specified in Article 18 paras. 1–5 ESA in connection with the provision of electronic services; those data include, for example, identification of the telecommunications terminal used by a user. Such data is defined as ‘internet data’ since it is related to internet services (see Art. 20c para. 1 of the Police Act of 6 April 1990⁷ – PA) such as internet access, email and internet telephony.

The legal bases on which law enforcement authorities (LEAs) may gather digital evidence are spread across several acts of law. The most important of these is the CCP, which also contains regulations on international cooperation in obtaining digital evidence located abroad. Another crucial act is the TL, which determines the scope of data that can be obtained, what entities are obliged to grant access to data and what entities are authorised to obtain data. This mainly concerns data retention and information transmitted over a telecommunications network. A third relevant act is the ESA, which concerns data and information in the possession of entities that provide electronic services. Finally, there is a set of provisions that regulate the activity of what are known as ‘authorised entities’ such as the police or the Internal Security Agency (ISA); those provisions also set out the authority of such entities to obtain digital evidence (see Section 14.3.2).

The LEAs act on the basis of those regulations in order to obtain electronic evidence. A distinction should be made between prosecutor’s offices and the courts, on the one hand, and other LEAs such as the police. In the latter case, it is vital to ensure that appropriate control mechanisms are in place when digital evidence is gathered. This has been pointed out by the Polish Constitutional Tribunal (CT), which attaches great importance to privacy, freedom of communication, the secrecy of correspondence and the protection of professional secrecy. The CT has stated that, with the growing importance of new technologies, there is an increased risk of their being used to violate the law. This justifies granting specialist bodies of public authorities, such as the police or state protection services, adequate authority enabling them to prevent and detect crime, prosecute perpetrators and provide information concerning threats to legally protected interests. A democratic state operating on the basis of the rule of law cannot ignore the increased importance of new technologies or the scale of their use, including for the purpose of breaking the law. In the opinion of the CT,

⁶ Act on the Provision of Electronic Services of 18 July 2002 (*ustawa o świadczeniu usług drogą elektroniczną*), consolidated text, Journal of Laws of 2020, item 344, as amended.

⁷ Police Act of 6 April 1990 (*ustawa o policji*), consolidated text, Journal of Laws of 2021, item 1882, as amended.

not providing the police and state protection services with the possibility of using advancements made in modern technology, or providing them with such a possibility but within an inadequate scope, may mean a failure on the part of the state to discharge its constitutional duty to guarantee the safety of citizens (Article 5 Constitution of the Republic of Poland), or may violate the principle of the effectiveness of public institutions.⁸

In this way, the CT pointed to the need to ensure appropriate regulations that allow the police to use modern methods of gathering evidence while at the same time guaranteeing that citizens' rights in such cases remain protected (see Section 14.3.4). Following this judgment, however, no changes were made to the CCP or the TL, but changes were made, for example, to the law on the police.

14.1.2 Data Retention Obligations: Legal Framework, Practice and Challenges

Under Polish law, there are binding regulations concerning data retention obligations. These are laid down in Articles 180c to 180d TL, and result from the implementation of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Directive 2006/24).⁹ The provisions of the Directive were implemented in Polish law through an amendment to the TL of 24 April 2009.¹⁰

However, in the case of *Digital Rights Ireland*, the Court of Justice of the EU (CJEU) invalidated the Directive.¹¹ Still, the Polish TL remains substantially unchanged. Even more interestingly, after the CJEU judgment, in a judgment of 30 July 2014, the CT addressed the issues of data retention, correspondence interception and wiretapping.¹² The CT explained that the statutory provisions contested in the case, which regulate the conditions for providing intercepted telecommunications data to competent services, do not directly constitute the implementation of Directive 2006/24/EC, and therefore the CJEU judgment of 8 April 2014 is not directly binding on the CT when assessing the constitutionality of national regulations.¹³

In practice, of course, since Directive 2006/24/EC was annulled, there has been a discussion in the legal doctrine on the application of the TL in the field of data retention.¹⁴ After a number of judgments of the CJEU, in particular those of 21 December 2016, *Telez Sverige AB przeciwko Post- och telestyrelsen*,¹⁵ and 5 April 2022, *G.D. przeciwko The Commissioner of the Garda*

⁸ Judgment of the Polish Constitutional Tribunal (*Trybunał Konstytucyjny*) of 30 July 2014, K 23/11, *Orzecznictwo Trybunału Konstytucyjnego* A 2014, No. 7, item 80, <http://trybunal.gov.pl>.

⁹ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, [2006] OJ 105, 15 March 2006, 54.

¹⁰ Act on an Amendment of the Telecommunications Law and certain other Acts of 24 April 2009 (*ustawa o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw*), Journal of Laws of 2009, No. 85, item 716.

¹¹ Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and others and Kärntner Landesregierung and others* [2014] ECLI:EU:C:2014:238.

¹² Judgment of the Constitutional Tribunal of 30 July 2014.

¹³ See, e.g., Judgment of the Constitutional Tribunal of 30 July 2014, 65.

¹⁴ See P. Brzeziński, 'Glosa do wyroku Trybunału Sprawiedliwości z dnia 21 grudnia 2016 roku w sprawach połączonych C-203/15 I C-698/15', in B. Opaliński and M. Rogalski (eds.), *Kontrola korespondencji. Zagadnienia wybrane* (Warsaw: Oficyna Wydawnicza Uczelni Łazarskiego, 2018), 76–84; M. Rogalski, 'Are the Regulations with Respect to the Retention and Provision of Communications Data Appropriate in Poland? A Proposal for Changes' (2015) 2 *Ius Novum* 229–231.

¹⁵ Joined Cases C-203/15 and C-698/15, *Telez Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others* [2016] ECLI:EU:C:2016:970.

Síochána i in.,¹⁶ the current Articles 180c to 180d TL must be deemed contrary to Articles 7, 8, 11 and Article 52 para. 1 of the Charter of Fundamental Rights of the European Union (CFREU).¹⁷ Articles 180c to 180d TL are of a general nature and do not foresee distinctions being made, that is, they permit the retention of all traffic and location data of all subscribers and registered users of all means of electronic communication, and do not restrict access to such data solely for the purposes of combating serious crime.

In order to implement Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code¹⁸ in the Polish legal order, new legislation has been prepared – the Electronic Communication Law.¹⁹ The draft law is expected to enter into force in the first half of 2023. The provisions of the draft concern not only telecommunications companies and the provision of telecommunications services but also electronic communications companies and the provision of electronic and interpersonal communications services. Relevant amendments have therefore been made to the provisions on gathering and granting access to telecommunications data.

14.1.2.1 Scope of Data Covered by Data Retention

Pursuant to Article 180c para. 1 TL, data must be retained if it is necessary in order to:

- (1) identify the network termination, telecommunications terminal equipment and end user:
 - (a) initiating a call, (b) to whom the call is directed; or (2) determine: (a) the date, time, and duration of a call, (b) the type of connection, or c) the location of the telecommunications terminal equipment.

Pursuant to Article 180d TL, telecommunications companies are obliged to ensure, at their expense, that authorised entities (e.g. the police, a court or a prosecutor) can access and copy data processed by the company in connection with the telecommunications services it provides, as specified as follows:

- transmission data, meaning data processed for communication or invoicing purposes, and including location data, that is, all data indicating the geographical location of the end device of a user of publicly available telecommunications services;
- data on attempts to connect between network terminations, including data concerning unsuccessful connection attempts, data signifying connections between telecommunications terminal devices, or network terminations that have been set up but not received by the end user, or connections that were terminated;
- user surnames and first names;
- user parents' names;²⁰
- user place and date of birth;
- user residential address (and mailing address if different from residential address);
- PESEL (i.e. national ID number in the case of citizens of the Republic of Poland);

¹⁶ Case C-140/20, *G.D. v. The Commissioner of the Garda Síochána and others* [2022] ECLI:EU:C:2022:258.

¹⁷ Charter of Fundamental Rights of the European Union, [2012] OJ C 326, 26 October 2012.

¹⁸ Directive: Directive 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code, [2018] OJ L321, 17 December 2018, 36–214.

¹⁹ The most recent version of the draft is from 5 May 2022 Electronic Communication Law (*prawo komunikacji elektronicznej*), https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/576666_projekt-ustawy-prawo-komunikacji-elektronicznej.html.

²⁰ Since there may be users who have the same surname and given names, having their parents' names makes it possible to distinguish between them.

- name, series and number of documents confirming user identity and, in the case of foreign nationals who are not nationals of a member state or the Swiss Confederation, passport or residence card number;
- documents confirming the legal capacity to incur liabilities towards a provider of publicly available telecommunications services resulting from a contract for the provision of telecommunications services;
- data from an electronic list of subscribers, users or network terminals, which also includes data obtained upon the conclusion of a contract, where the list is maintained by a telecommunications company providing publicly available telecommunications services.

14.1.2.2 Entities Obligated to Collect and Retain Data

In accordance with the TL, public telecommunications network operators and providers of publicly available telecommunications services are obliged to retain telecommunications data. Pursuant to Article 2 para. 27 TL, ‘telecommunications company’ means a company or other entity authorised to do business based on other provisions and which provides telecommunications and related services. A telecommunications company authorised to provide telecommunications services is called a ‘service provider’; an ‘operator’ offers a public telecommunications network or related services. This division into operators and service providers is very important with regard to the fulfilment of the data retention obligations being discussed here: while operators have adequate organisational and technological resources to fulfil these obligations in practice, telecommunications providers are quite often small businesses, or even sole entrepreneurs. They may not have the means necessary to ensure that they can discharge the duties imposed by the law, for example to purchase appropriate software for registering and gathering data, since the costs involved could amount to several years of such a company’s revenue. Requiring all telecommunications entities to meet those obligations to such a broad extent, regardless of their real capacity and resources, can be onerous for service providers.

A public telecommunications network is a telecommunications network used mainly for the purpose of offering publicly available telecommunications services (Art. 2 para. 29 TL). The term ‘publicly available telecommunications service’ means a telecommunications service available to the general public, that is, to everyone (Art. 2 para. 31 TL).

14.1.2.3 Data Retention Period

In accordance with Article 180a para. 1(1) TL, public telecommunications operators and providers of publicly available telecommunications services are obliged, at their own expense, to collect and retain data generated in the telecommunications network, or which they process in the territory of the Republic of Poland, for a period of twelve months following the date of connection or an unsuccessful connection attempt; on the date when that period ends, they must destroy the data, except for data that is protected by law. The twelve-month retention period is independent of the type of offence or the penalty concerned, unlike wiretapping, which may be legally used in Poland only in connection with the most serious crimes enumerated in the CCP. The TL allows for a longer data retention period, but for different purposes. In accordance with Article 168 TL, a publicly available telecommunications services provider is obliged to record data concerning telecommunications services provided for the purpose of

calculating charges and dealing with complaints. Such data must be retained for at least twelve months or, in the case of a complaint, for the time necessary to resolve the dispute.

Article 180a para. 1 pt. 1 TL concerns the retention and storage of data generated in a telecommunications network or processed by an operator or a service provider. The regulations apply to telecommunications companies entered in the registry of telecommunications enterprises maintained by the regulator (Office of Electronic Communication, OEC) that provide telecommunications services in the territory of Poland – meaning the place where data generated during the provision of a given service in Poland is actually stored. Where doubts arise, the criterion of the data being located in Polish territory is decisive; in the case of entities providing services based on the ESA, the location is defined in a similar manner. In a situation where the service provider and/or data subject are located in the territory of Poland but the data is stored abroad, the European Investigation Order (EIO) is used.

14.1.2.4 Entities Authorised to Request Telecommunications Data

The following entities may request access to telecommunications data for the purposes of proceedings they conduct, specifically criminal proceedings: courts, public prosecution offices, the police, the Internal Supervision Bureau, the Border Guard, the State Protection Service, the ISA, the Military Counterintelligence Service, the Military Police, the Central Anticorruption Bureau and the National Revenue Administration. These entities listed are known as ‘authorised entities’ (*uprawnionymi podmiotami*) (Art. 179 para. 3 pt. 1(a) TL). The conditions for access are defined in statutes; in general, they depend on whether the data is made available in the context of a criminal case or as part of operations performed by the police or another authorised entity.

14.1.2.5 Complaints Against the Unlawful Gathering and Storage of Telecommunications Data

When analysing the possibilities of judicial redress available to individuals whose data has been unlawfully retained or used, it is necessary to distinguish between data retained by a court or a prosecutor in accordance with the CCP and data retained pursuant to the legal acts regulating the operations of other authorised entities, for example the police.

Where telecommunications data is provided at a court’s or a prosecutor’s request in the course of criminal proceedings, the request sent to the relevant telecommunications company should also be delivered to the telecommunications services subscriber whose list of telecommunications connections or other transmissions of information were provided. The delivery of the decision may, however, be postponed for a fixed period necessary for the case, but only until a legally binding judgment is handed down on the merits of the case (Art. 218 § 2 CCP). Otherwise, that is, if the person concerned were to be informed about the collection and provision of their data, the data collection would be ineffective since that person would then be careful about whom they contacted and how. When the delivery of a decision is postponed, obviously the person concerned cannot appeal against it because they are unaware that their data was made available. They can only appeal after receiving the decision, which, as already stated, must be delivered before the time the proceedings are concluded.

The legal acts regulating the operations of authorised entities other than the courts or prosecutors also provide another mode of supervision. The provisions of the PA that regulate police access to telecommunications data provide an example of this. Article 20ca PA regulates the judicial supervision over access to telecommunications data. Pursuant thereto, the district

court having jurisdiction over the headquarters of the police unit to which telecommunications or internet data has been made available must supervise the manner in which it was obtained. The police provide the district court with semi-annual reports, particularly concerning the number of cases where telecommunications or internet data was obtained, with a legal classification of the offences related to which data was made available. In this scope, a critical view should be taken of the PA, for control over data access is exercised only after the data has been provided, not before. It is therefore not possible to react in advance to any potential abuse or to refuse consent to the data being provided. In this sense, the PA may violate Articles 7, 8 and 11 and Article 52 para. 1 CFREU. In its jurisprudence, the CJEU has pointed to the need to obtain the prior consent of a court or other independent body to data being made available²¹ (see Section 14.3.4).

14.2 TERMINOLOGY AND CATEGORISATIONS

14.2.1 *Data*

14.2.1.1 Terminology

There is no single definition of ‘data’ in Polish criminal law; two definitions exist. In substantive criminal law, the term ‘computer data’ appears, while in procedural criminal law ‘telecommunications data’ appears (Article 218 CCP). For example, Article 268a CC, which concerns the destruction of IT data, uses the term ‘computer data’. In accordance with Article 268a § 1 CC, ‘whoever, not being authorised to do so, destroys, damages, deletes, alters or prevents access to computer data, or substantially disrupts or prevents the automatic processing, retention or provision of such data, is subject to a penalty of deprivation of liberty for up to three years’. Computer data is here conceived broadly as any data obtained and processed in an information system. The concept of ‘computer data’ used in the CC is defined in accordance with Article 1(b) of the Convention of the Council of Europe of 23 November 2001 on Cybercrime (CC Convention)²² as ‘any representation of facts, information or concepts in a form suitable for processing in a computer system, including a suitable program resulting in the performance of a function by a computer system’.

The current content of Article 218 CCP is a consequence of an amendment to the CCP²³ introduced several years ago. Article 218 CCP now refers to the definition of data contained in the TL. Previously, the same article spoke of ‘a list of telecommunications connections or other transmissions of information, including correspondence sent by electronic mail, considering the time of a connection and other data related to the connection or transmission that do not constitute the content of a telephone conversation or other transmission of information’. That amendment of Article 218 CCP is the result of the implementation of Directive 2006/24.

The two concepts just mentioned are used in various contexts: ‘telecommunications data’ in connection with the retention and provision of telecommunications data (‘telecommunications data retention’) and ‘computer data’ in connection with offences against information systems

²¹ See Joined Cases C-512/18 and C-520/18, *La Quadrature du Net i in.* [2020] EU:C:2020:791, para. 189 and jurisprudence there referred to, and Case C-746/18, *Criminal proceedings against H. K.* [2021] ECLI:EU:C:2021:152, paras. 51–52.

²² Council of Europe, *Convention on Cybercrime*, ETS No. 185, 23 November 2001.

²³ Act on an Amendment of the Telecommunications Law and certain other Acts of 24 April 2009 (*ustawa o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw*), Journal of Laws No. 85, item 716.

(przestępstwa przeciwko ochronie informacji). The lack of a single definition of data, at least in criminal law, does not facilitate application of the relevant provisions in practice. Article 218 § 1 CCP uses the term ‘data’ by referring to Articles 180c and 180d TL, which precisely indicate what kind of data is meant. In the case of Article 241 CCP, there is no such precision. Here, three concepts are used: ‘content of other conversations’, ‘transmission of information’ and ‘correspondence sent via electronic mail’. None of these is defined by the CCP, which leads to divergent interpretations and understandings.²⁴

Finally, it should be noted that, in the Personal Data Protection Act,²⁵ the concept of ‘personal data’ is used, though for another purpose – data protection. The definitions of ‘computer data’ and ‘telecommunications data’ differ from other related definitions, such as that of ‘personal data’.

14.2.1.2 Categorisation

The CC Convention lays down three data categories: computer data (Article 1b), traffic data (Article 1d) and content data (Article 21). The concept of computer data was introduced into the CC for the purpose of describing offences against information systems (Chapter XXXIII CC), and to the CCP within the scope of securing and granting access to such data (Article 218a CCP). The other two categories were introduced into the TL and, by means of references in the provisions of the CCP to the TL, are also used in criminal proceedings. Article 218 CCP refers to Articles 180c and 180d TL on subscriber data and location data (see Section 14.1.2.1). The latter provisions determine what data can be classified as ‘traffic data’ in the meaning of Article 1(d) CC Convention, namely, the time and date of a connection or transmission data, meaning data processed for the purpose of transmitting announcements in telecommunications networks (Article 159 para. 1(3) TL). The concept of ‘content data’ coincides with the definition of ‘telecommunications transmission’ (Article 2 pt. 27a TL).

‘Telecommunications data’ (Articles 180c–d TL), understood as data concerning a user, movement or location, should be distinguished from ‘telecommunications transmission’. In accordance with Article 2 pt. 27a TL, ‘telecommunications transmission’ means the content of telephone conversations or other information sent over a telecommunications network. The definition of telecommunications transmission was added as an amendment to the TL of 24 April 2009 in order to regulate the rights of courts, prosecutors and other authorised entities to access and record telecommunications transmissions. The concept of telecommunications transmissions as defined in the TL is used in statutes regulating the rights of those bodies, for example in the PA.²⁶ Telecommunications companies are obliged to record telecommunications transmissions for the needs of courts and prosecutors (Art. 179 para. 2 pt. 2 TL). This applies to all information transmitted via a telecommunications network. Such data can also be referred to as content data.

Chat rooms should be included within this scope. Pursuant to Article 2 para. 27a TL, the term ‘telecommunications transmission’ encompasses the content of telephone conversations and other information transferred via telecommunications networks, including emails, text messages, text content and so on. The same concept is used in other acts regulating correspondence

²⁴ More at M. Rogalski, *Kontrola korespondencji* (Warsaw: C. H. Beck, 2016), 101–114.

²⁵ Act of 10 May 2018 on the Protection of Personal Data (*ustawa o ochronie danych osobowych*), Journal of Laws of 2018, item 1000.

²⁶ For further analysis, see S. Piątek, *Prawo telekomunikacyjne. Komentarz* (Warsaw: C. H. Beck, 2013), 70–71.

interception and wiretapping, and also extends to communication that takes place in the context of online games.

With regard to internet protocol (IP) history/dynamic IP addresses, attention should be drawn to the provisions of the ESA. Pursuant to Article 2 pt. 1 ESA, an electronic address is an IT system designation that enables communication by electronic means, specifically electronic mail. An IT system is a group of IT devices and software that function together to provide data processing and storage, as well as data transmission and collection, through telecommunications networks using a terminal device appropriate to the type of telecommunications network in the meaning of the TL (Art. 2 pt. 3 ESA). Article 1(a) CC Convention defines ‘computer system’ as every device of a group of joint or mutually connected devices one or more of which, in compliance with the program, performs automatic processing of data. The concept of ‘computer system’ is narrower than the concept of a telecomputing system (which extends to telecommunications). Telecomputing system (information and communication technology (ICT) system) means a set of cooperating IT devices and software ensuring processing, storage as well as sending and receiving of data via telecommunications networks (see Art. 3 para. 3 of the Act of 17 February 2005 on the IT Activity of Entities Implementing Public Tasks²⁷).

14.2.2 *Service Providers*

In particular Polish regulations, different definitions appear of entities that provide telecommunications services or electronic services. As a rule, the legal act concerning the provision of particular services contains a definition of those services for the purposes of the act.

Pursuant to the binding provisions of Article 2 pt. 27 TL, a telecommunications company is a company or other entity authorised under separate regulations to do business and that conducts economic activity consisting in the offering of telecommunications networks, associated services or telecommunications services. A telecommunications company authorised to provide telecommunications services is called a ‘service provider’; one authorised to provide public telecommunications networks or associated services is called an ‘operator’. So, in the TL two definitions are used: operator and service provider. In EU directives, when discussing matters concerning electronic communication, reference is made to companies providing electronic communications networks and services. This expression is not defined, however, in the directives. Under EU law, a functional concept of company is used, according to which a company is any entity conducting business activity, regardless of its legal form, the role of profit in its activity or how it is financed.²⁸

Article 2a of the Electronic Commerce Directive²⁹ defines the concept of ‘information society service’ as a service within the meaning of Article 1(2) of Directive 98/34/EC³⁰ as amended by Directive 98/48/EC.³¹ The Electronic Commerce Directive was implemented in the Polish legal system by the ESA. However, there is no single term that the Polish legislator uses in the various legal acts. For example, on some occasions we find ‘service’, on other occasions

²⁷ Act of 17 February 2005 on the IT Activity of Entities Implementing Public Tasks (*ustawa o informatyzacji podmiotów realizujących zadania publiczne*), consolidated text, Journal of Laws of 2021, item 2070, as amended.

²⁸ Piątek, ‘Prawo telekomunikacyjne’, 68–69.

²⁹ Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on Electronic Commerce’), [2000] OJ L 178, 17 July 2000, 1.

³⁰ Directive 98/34/EC of the European Parliament and Council laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society Services, OJ L 204, 21 July 1998, 37–48 (no longer in force).

³¹ Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, [1998] OJ L 217, 5 August 1998, 18–26 (no longer in force).

‘provision of electronic services’. Pursuant to the ESA, a ‘service provider’ means a natural person, legal person or organisational unit not having legal personality that conducts commercial activity or provides professional services, at least incidentally, using electronic means (Art. 2 pt. 6 ESA), whereas a service user means a natural person, legal person or organisational unit without legal personality that uses electronic services.

The concept of ‘internet access providers’ is not defined in Polish law at present, which makes the scope of the term unclear. In the TL, the term ‘service provider’ is used, while in the ESA we find the terms ‘providers’ or ‘users of services’. In practice, a number of other terms similar in meaning are used: ‘content providers’, ‘entities providing services on the Internet’ or ‘intermediary providers’.³²

There is also a group of what are known as digital service providers. On 6 July 2016, the European Parliament and the Council adopted Directive 2016/1148 (EU) concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).³³ In accordance with Article 4 of the NIS Directive, a digital service provider means any legal person that provides a digital service, that is, one that is paid for and provided at a distance via electronic devices and at an individual customer’s request, and that is also classified as an internet commercial platform, an internet search engine or a cloud processing service within the meaning of the NIS Directive. Thus, different categories of digital service providers can be distinguished: online marketplaces, online search engines and cloud computing services. The provisions of Article 4 NIS Directive define each category.

The provisions of the Directive were implemented in Polish law by the Act on the National Cybersecurity System of 5 July 2018 (NCS).³⁴ In accordance with Article 17 pt. 1 NCS, a provider of digital services can be a legal person or organisational unit without legal personality that has its registered office or management board in the territory of the Republic of Poland or that has a representative with an organisational unit in the territory of the Republic of Poland and that provides a digital service, with the exception of microbusinesses and small businesses as referred to in the Enterprise Law. Annex No. 2 to the NCS determines the types of digital services.

To conclude: at present, there are numerous definitions of entities that provide telecommunications services or electronic services. Some of those definitions originate from EU directives, others are used in the doctrine, and again others find their source in practice. Therefore, when a LEA decides to approach a given provider for particular data, it should check what legal act provides a basis for the provider’s operations; this will permit a proper legal definition of the provider, and will also make it possible to determine what obligations are imposed on the provider by that legal act.

14.3 DOMESTIC COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

14.3.1 Introduction

Cooperation between LEAs and service providers facilitates crime detection and prevention. Thus, LEAs often engage in this form of cooperation, especially because it is relatively simple to conduct and free of charge, that is, they do not have to pay private companies for the

³² See K. Chałubińska-Jentkiewicz and J. Taczowska-Olszewska, *Świadczenie usług drogą elektroniczną. Komentarz* (Warsaw: C. H. Beck, 2018), n. 34 to Art. 1.

³³ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ. L 194, 19 July 2016, 1–30.

³⁴ Act on the National Cybersecurity System of 5 July 2018 (*ustawa o krajowym systemie cyberbezpieczeństwa*), consolidated text, Journal of Laws of 2022, item 1863, as amended.

collaboration they require them to perform, because those activities result from legal obligations. Further, the law³⁵ does not limit requests for data to particular crimes only.

The law obligates both telecommunications operators and service providers to cooperate with LEAs. In practice, LEAs cooperate mainly with large telecommunications operators (in Poland, four major mobile operators and about a dozen stationary ones) – for several reasons. First, those operators have the largest customer bases (all mobile services customers in Poland are subscribers of the four mobile operators). Second, they have the technical, organisational and human resources needed to respond to law enforcement requests. Third, their cooperation with LEAs is well organised and runs smoothly. In the case of data other than telecommunications data that is not in the possession of telecommunications service providers or operators, such as data exchanges via websites or cloud computing services, this can be obtained from entities that possess it not only on the basis of the TL but also on the basis of the ESA (Art. 18). As explained in Section 14.2.1.2, the ESA regulates the provision of electronic services, which, pursuant to Article 2 pt. 4 ESA, means the performance of a service without the presence of the parties (remote communication) through the transmission of data at an individual customer's request, transmitted and received with the use of electronic processing, including digital compression, and the retention of data transmitted as a whole, received or transmitted with the use of a telecommunications network in the meaning laid down in the TL. It is therefore possible to distinguish telecommunications services from electronic services. The difference is rather conventional, however. The Polish legislator identifies the concept of the provision of electronic services in the meaning of Article 2(a) of Directive 2000/31/EC,³⁶ which adopts the definition of such services used in Directive 2015/1535/EU.³⁷ In turn, 'telecommunications service' means a service mainly involving the transmission of signals, including via a telecommunications network (Art. 2 pt. 48 TL). Thus, electronic services are provided in the same way as telecommunications services, through telecommunications networks.

The obligation to cooperate must be fulfilled by operators of public telecommunications networks and providers of publicly available telecommunications services operating in Poland, that is, those that are telecommunications companies registered with the OEC. Formally, under the wording of Article 10 TL, that obligation applies to all such entities registered and operating in Poland.

In other words, Poland has jurisdiction over data that is generated or processed by (Polish or foreign) service providers in the territory of Poland. The location of the service provider's headquarters is immaterial, as are the place of residence and the actual location of a suspect. If the location of data and/or a service provider and/or a data subject cannot be reasonably defined by a LEA at the moment a request to cooperate is made, the criterion of providing services in Poland is decisive (see Art. 179 TL and Art. 18 ESA).

In situations having one or more cross-border elements (e.g. a service provider and/or data subject located in the territory of Poland but data stored abroad), from a formal point of view, the national rules on direct cooperation with the service provider apply. However, the implementation of those rules will be problematic in practice because, for example, the service provider may not be able to fulfil the request if the server is located abroad as it will have limited legal access to the data. In such situations, there is an alternative solution – to apply the rules for mutual legal

³⁵ E.g., Art. 218 § 1 CCP or Art. 20c para. 1 pt. 1 PA.

³⁶ Directive on Electronic Commerce, 1–16.

³⁷ Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L 241, 17 September 2015, 1–15.

assistance (MLA) or, in intra-EU situations, the legal instruments that are based on mutual recognition, particularly the EIO.

When collecting or providing data, correspondence or post, Articles 218 or 218a CCP provide grounds for a request. In relation to computer data or computer system data that may be in the possession of any entity, Article 236a CCP read together with Article 217 CCP applies. Thus, the division concerns the type of data to be obtained: Article 218 CPC in the case of telecommunications data and Article 236a CCP in the case of computer data.

In accordance with Article 18 para. 6 ESA, a service provider must provide free access to information as referred to in Article 18 paras. 1–5 ESA to state bodies authorised under other provisions for the needs of the proceedings they conduct. For example, Article 18 para. 1 ESA enumerates the following data that a service provider may process and will have to grant access to: (1) a user's surname and given names; (2) the PESEL of a Polish citizen or, if the user does not have one, their passport number or other identification document number; (3) the user's place of permanent residence; (4) their correspondence address if different from the address referred to in (3); (5) the data used to verify the user's electronic signature; (6) the user's electronic address(es).

14.3.2 *Nature of Cooperation*

The legal basis for cooperation can be found in the following legal acts: (1) the CCP – all legal persons and natural persons are obliged to apply the provisions of criminal procedure in this respect; (2) the acts regulating the activities of entities authorised to request data (e.g. in the case of the police, the PA); (3) the TL, which defines the obligations of telecommunications entities, including service providers; (4) the ESA. In general, those legal grounds are divided into two groups: first, the provisions of the CCP and special acts, for example the PA and the Central Anticorruption Bureau Act, and second, the TL and the ESA. The first group determines the rights of courts, public prosecutors and the police to request data. The second group determines companies' obligations to provide them. Whether the provisions of the CCP or special acts are to be applied depends on a particular public authority's competence and its duties resulting from those provisions. For example, a prosecutor will request data in accordance with the CCP in conjunction with the TL, while the police act on the basis of the PA, and may also refer to the TL.

Cooperation in Poland is mandatory. The existence of a legal obligation to cooperate means that, where there are legal grounds for obliging an entity to cooperate, failure of the entity to do so may result in a penalty being imposed. Legal sanctions in the form of financial administrative penalties are laid down in the provisions of the TL. An unjustified refusal (i.e. one without legal grounds) by a service provider to cooperate constitutes violation of the TL (Art. 209 para. 1 pt. 10 TL) and may result in: (a) a fine of up to 10 per cent of the provider's yearly net income; (b) a fine imposed on the manager of the service provider of up to three months of their salary; (c) in the worst case, being deleted from the register of telecommunications enterprises, meaning that the service provider must cease operating.

The penalties foreseen in Articles 285 and 287 CCP may also be imposed on persons, and in particular on employees of a company who fail to perform activities related to data in the possession of their company. Pursuant to Article 285 § 1 CCP, if an expert fails to respond to a summons by an authority conducting proceedings, a penalty of up to PLN 3,000 (ca. €700) may be imposed; pursuant to Article 287 § 1 CCP, Article 285 § 1 CCP is applicable by analogy to a person who unlawfully fails to perform a 'specialist' act, for example appearing before a court as an expert employee of a company summoned to explain why certain data in its database cannot

be made available for technical reasons. Article 287 § 1 CCP also concerns representatives or directors of an institution, legal person or organisational unit without legal personality who are obliged to provide assistance to an authority conducting criminal proceedings, such as the police or a prosecutor's office, and who groundlessly fail to provide assistance to that authority within the time period it has specified.³⁸

When obtaining data, a LEA must do so in accordance with the provisions of the CCP and the TL, otherwise there would be a serious infringement of the law. If data is obtained in violation of the law, its admissibility in a criminal trial is always assessed by the courts. A few years ago, such evidence was always rejected. Currently, after amendments to Articles 168a and 168b CCP,³⁹ this is no longer so. The courts shall judge. In this respect, two provisions of the CCP are worthy of note. First, pursuant to Article 168a CCP, evidence cannot be declared inadmissible only because it was obtained in violation of the provisions regulating the procedure or by means of a forbidden act as referred to in Article 1 § 1 CC, unless that evidence was obtained by a public officer in the course of performing their duties as a result of the commission of murder, deliberate harm to a person's health or deprivation of liberty. Second, pursuant to Article 168b CCP, if, as a result of an operational control conducted at the request of an authorised entity, evidence is obtained showing that the person against whom the operational control was conducted committed another crime being investigated other than that covered by the operational control, the prosecutor decides whether that evidence may be used in criminal proceedings. Clearly, these new legal provisions are aimed at permitting evidence to be gathered even in situations where it was obtained in violation of the rules of criminal procedure or by means of a prohibited act. The court will evaluate the evidence, but only during trial, after the prosecutor has sent the case to the court.

Some doubts may arise concerning the fulfilment of the obligations stipulated in Article 18 para. 6 ESA. In a resolution of 30 September 2014, which was the answer to the legal question of the lower court (Article 441 CCP),⁴⁰ the Supreme Court explained that Article 18od TL (which stipulates that telecommunications companies are obliged to ensure conditions of access and retention and to grant access to data they process to authorised entities, courts and prosecutors, at the company's own expense) applies to data related to telecommunications companies' service of transmitting electronic mail. It does not apply, however, to a service provider granting state bodies access to data for the needs of proceedings they conduct within the scope set out in Article 18 para. 6 ESA. Here, the sanctions laid down in the TL do not apply. On the other hand, the ESA does not lay down any legal sanctions for such infringements. In the case, then, where an entity providing electronic services refuses to grant access to data as referred to in Article 18 paras. 1–5 ESA (e.g. the electronic address of a user), authorised state bodies as referred to in Article 18 para. 6 EPA will be able to demand that data on the basis of and under the procedure provided in separate provisions. Examples of this are Article 218a § 1 CCP, which permits IT data to be secured at the demand of a court or a prosecutor, and Article 217 § 1 CCP, pursuant to which things that can constitute evidence in a case – things such as information carriers – must be handed over upon a request by a court or prosecutor or, in urgent cases, by the police.

As stated earlier, in Poland cooperation is mandatory. In practice, informal cooperation, that is, that which is voluntary and not stipulated by any provision of the law, is very rare because

³⁸ More at Rogalski, 'Kontrola korespondencji', 316 *et seq.*

³⁹ The Act on an Amendment of the Code of Criminal Procedure and certain other acts of 11 March 2016 (*ustawa o zmianie ustawy – kodeks postępowania karnego oraz niektórych innych ustaw*), Journal of Laws of 2016, item 437.

⁴⁰ Polish Supreme Court (*Sąd Najwyższy*), 30 September 2014, I KZP 18/14, item 86.

entities are not willing to provide data or information lest they be accused of having done so unlawfully. The provision of data without legal grounds may be treated as unauthorised violation of privacy. Such data may be used as evidence in proceedings, but the legality of how the data was obtained will be evaluated by the court. Similarly, in a situation where an entity possesses data, for example data stored abroad, and is not legally bound by the provisions of Polish law to make the data available to a LEA but decides to do so voluntarily under the procedure of the ESA, the LEA will be able to present that data in the proceedings, and the court will evaluate it to determine whether it should be admitted as evidence.

The law determines when and under what circumstances a service provider is obliged to cooperate with a LEA, and so, provided a request is based on the law, the service provider must cooperate. Only if there are no legal grounds for the request, or if the grounds are incorrect or unclear, can a service provider refuse to provide data. In practice, such refusals rarely occur. If a request lacks certain data, it is normally returned or the entity is asked to supplement it. Importantly, though, the entity providing data, that is, the telecommunications company, does not assess the content of a request.

In the event that a response to a request is incomplete or provided in the incorrect form, the LEA will ask the service provider to correct its response. If there are still deficiencies in the answer provided, the LEA may apply to the OEC for the imposition of a penalty. Service providers can ask a LEA for additional information that will allow them to properly fulfil the LEA's request. Service providers cannot provide access to data conditionally, for example on the condition that it not be used as evidence.

In practice, refusals to cooperate occur only where there are no legal grounds for the request, the request is made from an unauthorised entity, the request is technically or organisationally impossible to fulfil, or the service provider does not possess the data requested. Service providers do not assess the scope of requests or types of request. There is no cost issue because data must be made available free of charge. In specific cases, a refusal may occur when, for example, a service provider does not possess data concerning the requested period (e.g. the data was subject to retention for one year and the request concerns data from two years back). There are also situations in which data is requested by an unauthorised entity, for example a civil law court hearing a divorce case (as a rule, only criminal courts can request data).

14.3.3 *Overview of Existing Cooperation Duties*

The mode in which data is obtained depends on the type of data and the entity that is to provide it. In the case of traffic data, as referred to in Articles 180c and 180d TL, Article 218 CCP applies; it obliges a telecommunications company to issue traffic data upon a request contained in a decision issued by a court or prosecutor. The decision sets out the scope and type of data to be produced. Pursuant to Article 218 § 1 CCP, such data should be provided when 'they are significant for a pending proceeding'. In the case of IT data stored on a data carrier or in an IT system, Article 218a CCP applies (see Section 14.3.2); it obliges entities conducting telecommunications activity to secure such data upon a request by a court or prosecutor. Those entities should also make IT data they possess in IT systems or devices available under the procedure of Article 236a CCP (see Section 14.1.1). Moreover, they should make available information transfers, including correspondence sent by electronic mail, under the procedure of Article 241 CCP (see Section 14.1.1). Finally, entities providing electronic services should grant access to data as referred to in Article 18 paras. 1–5 ESA (Art. 18 para. 6 ESA; see Section 14.3.1 of this chapter). Pursuant to Article 18 para. 5 ESA, a service provider may process data that characterises a customer's use of electronic services

(‘exploitation data’), for example information concerning the initiation, completion and scope of every single use of electronic services, or designations identifying the end device of the telecommunications network of a telecomputing system used by a customer. Thus, Article 18 ESA determines what other data may be made available when electronic services are provided based on the provisions of that Act. This comprises data other than telecommunications data connected along with the provision of telecommunications services, for example voice services. It should be emphasised that all evidence obtained in this way is admissible in court, but will always be subject to judicial assessment, especially as regards the method by which it was obtained.

Apart from the provisions of the CCP, LEAs may obtain data on the basis of the laws regulating their activities, which provide them with similar entitlements – for example the police and the ISA. For example, pursuant to Article 19 para. 6 PA, surveillance is conducted in a covert manner and consists specifically in: using technical means, including telecommunications networks, to obtain and record the content of conversations; obtaining and recording the content of correspondence, including correspondence sent using electronic means of communication such as email; and obtaining and recording data stored or contained on data carriers, telecommunications end devices and computer and telecomputing systems. These provisions may constitute a basis for requesting data from, for example, a computer/online security system provider, a webpage, a chat room or application administrator or an online currency exchange service.

Article 20c PA states that, in order to prevent or detect offences, save human life or health, or support search and rescue operations, the police may obtain ‘internet data’, that is, data that does not constitute a telecommunications transfer or a transfer within the provision of electronic services as laid down, inter alia, in Article 18 paras. 1–5 ESA, and, further, that the police may process such data without the knowledge or consent of the person involved. The Chief Commander of the police or a provincial chief of police passes on data relevant to criminal proceedings to the competent prosecutor, who will decide on how it may be used. Data that is irrelevant to the criminal proceedings should be immediately destroyed (Art. 20c para. 7 PA).

All data should be properly secured. Moreover, LEAs may collect and keep data only for the length of time necessary to conduct the criminal proceedings. After that period, the data should be destroyed immediately under the supervision of a commission (Art. 20c para. 7 PA). How data should be destroyed is set out in the implementing acts to the laws that govern the activities of authorised entities, such as the police. An example of this is the Regulation of the Minister of the Interior and Administration concerning the method of documenting police surveillance, the retention and provision of conclusions, orders and materials obtained as a result of the application of surveillance, as well as the processing and destruction of such materials of 10 June 2011,⁴¹ which was issued based on Article 19 para. 21 PA.⁴² Under § 7 of that Regulation, the documented destruction of materials that do not contain evidence making penal proceedings possible, or that have no relevance to pending criminal proceedings, or that were gathered during a control conducted by the police in the case where a court has not consented to the continuation of the proceedings, is performed by a permanent or an ad hoc commission.

⁴¹ The Regulation of the Minister of the Interior and Administration on the method of documenting operational control by the police, storage and transmission of applications, orders and materials obtained during the application of this control, as well as the processing and destruction of such materials of 10 June 2011 (*Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie sposobu dokumentowania prowadzonej przez policję kontroli operacyjnej, przechowywania i przekazywania wniosków, zarządzeń i materiałów uzyskanych podczas stosowania tej kontroli, a także przetwarzania i niszczenia tych materiałów*), Journal of Laws No. 122, item 697, as amended.

⁴² The Police Act of 12 February 2007 (*ustawa o policji*), Journal of Laws of 2007, No. 43, item 277, as amended.

As to whether service providers can be ordered to infringe security measures and/or decrypt data, it should be noted that, by law, those obligations rest on the service provider, that is, the entity providing a given service should fulfil its obligations to authorised entities. There are two such situations: the first is when a provider offers encrypted services. Here, the codes to be decrypted must be available to LEAs before the service provider launches its commercial offer employing security or encryption. Further, the service provider is obliged to decrypt data requested. The second situation is when a given service provider's customer uses the solutions of another entity that has encrypted their data. Here, the service provider does not have to decrypt the data. In other words, in the first situation, where an entity offers decrypted services for which it is responsible because it developed them on its own but cannot decrypt the data at an authorised entity's request, it has not fulfilled its obligations towards the authorised entity.

14.3.4 *Legal Remedies and the Protection of Fundamental Rights*

The provisions regulating cooperation between service providers and LEAs take into account a series of important constitutional values (e.g. privacy), but at the same time aim to ensure the effectiveness of criminal law enforcement. In order to establish to what extent the present regulations efficiently protect citizens' rights in the area of data retention, it is necessary to explain the following issues and to make certain distinctions. Although recently there have been adverse changes in the CCP that permit the use of evidence obtained in violation of the law (Art. 168a CCP, discussed in Section 14.3.2.), it is the court that always evaluates the evidence and takes the final decision. The provisions of the CCP also provide for the submission of complaints against measures taken. Pursuant to Article 236 § 1 CCP, persons whose rights have been infringed (e.g. due to a legally flawed seizure of carriers containing electronic data or the unlawful obtainment of telecommunications data) have the right to submit a complaint against those measures. The district court having jurisdiction over the area where the proceedings are conducted hears complaints about decisions issued in investigation.

The regulations concerning entities other than a court or a prosecutor's office, such as the police, should be assessed much more critically. In its jurisprudence, the CT has indicated a need to ensure appropriate regulations that allow the police to use modern techniques of gathering evidence but which at the same time guarantee that citizens' rights are protected when evidence is gathered⁴³ (see Section 14.1.1). This led to an amendment of the PA, with regulations introduced on how evidence may be gathered, particularly pertaining to ensuring control by the courts that data are obtained lawfully, retained only for the period necessary for the purposes of the proceedings and destroyed in a documented manner at the end of that period. Before those changes, the police could, for example, retain data for an unlimited period of time, even if the data were no longer needed for the proceedings under which they were obtained. This created a risk of such data being used for other purposes.

Regarding infringements of the provisions regulating data collection and access, first, it must be proved that the provisions of law determining the conditions for collection and access have been violated. Civil claims against the State Treasury (represented by the entity that violated the law) can then be pursued through litigation. In practice, such cases are very rare. Another way of a civil claim being brought during the course of criminal proceedings is provided in Article 46 § 1 CC, pursuant to which, in the case of a conviction, the court may rule – and at the aggrieved party's or another entitled person's request, the court shall rule – that all or part of the damage

⁴³ Constitutional Tribunal judgment of 30 July 2014, K 23/11, 51–52.

caused as a result of the offence committed must be redressed, or that the offender must pay damages for the harm caused.

14.4 CROSS-BORDER COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

14.4.1 Introduction

Issues related to cross-border cooperation between LEAs and service providers are regulated in the provisions of the Polish CCP and mutual legal assistance treaties (MLATs). Chapters 62a–d CCP are the implementation of Articles 25–34 CC Convention, which, after being ratified, entered into force in Poland on 1 June 2015 (Art. 36 § 4 CC Convention). Currently, a process is underway in Poland to ratify a second additional protocol to the CC Convention⁴⁴ in order to enhance cooperation and the disclosure of electronic evidence. Its implementation in the Polish legal order (in the CCP and possibly in domestic legislation on the cybersecurity system) will put an end to the need for entities to meet requirements without a legal basis, such as, for example, that of complying with the deadlines for executing an order to obtain specific information or data.

The provisions of Chapter 62a and 62b CCP concern member states requesting or being requested to execute a decision on production of retained data, whereas Chapter 62c and 62d CCP concerns a member state requesting or being requested to carry out evidentiary actions based on an EIO. Chapter 62a (Art. 589g–589ka) and 62b (Art. 589l–589v) was added to the CCP by an amendment of 7 July 2005⁴⁵ due to the need for Poland to meet its international commitments, and specifically to implement Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (Decision 2003/577/JHA),⁴⁶ later replaced by Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders (Regulation 2018/1805).⁴⁷

Chapter 62c and 62d was introduced to the CCP on the basis of the Act of 10 January 2018 amending the Code of Criminal Procedure and Other Acts⁴⁸ in order to implement Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigative Order in criminal matters (Directive 2014/41/EU),⁴⁹ even though EU member states were obliged to take the measures necessary to implement the provisions of that Directive by 22 May 2017 (Article 36 Directive 2014/41/EU). The provisions of Chapter 62c and 62d CCP replace the previous mechanisms of cooperation that initially functioned on the basis

⁴⁴ Proposal for a Council Declaration authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, [2021] COM/2021/719 final, 25 November 2021.

⁴⁵ Act of 7 July 2005 on an amendment of the Code of Criminal Procedure and the Code of Procedure in Cases of Misdemeanour (*ustawa o zmianie ustawy – kodeks postępowania karnego oraz ustawy – kodeks postępowania w sprawach o wykroczenia*), Journal of Laws No. 143, item 1203.

⁴⁶ Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, [2003] OJ 196, 2 August 2003, 45.

⁴⁷ Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders, [2018] OJ L 303, 28 November 2018, 1.

⁴⁸ Act of 10 January 2018 amending the Code of Criminal Procedure and Other Acts (*ustawa o zmianie ustawy – kodeks postępowania karnego oraz niektórych innych ustaw*), Journal of Laws of 2018, item 201.

⁴⁹ Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, [2014] OJ L 130, 1 May 2014, 1.

of Decision 2003/577/JHA. They do not, however, replace the existing mechanism for cooperation carried out on the basis of Chapter 62a CCP in relation to EU member states not connected with Directive 2014/41/EU.

14.4.2 *Cooperation of National LEAs with Foreign Service Providers*

14.4.2.1 Legal Framework

In Poland, the cooperation between Polish LEAs and foreign service providers is of an indirect nature. Within the EU, access to data held by foreign service providers⁵⁰ is based on mutual recognition instruments (in particular the EIO) and MLATs, and requires intervention by the authorities of the country where the service provider is located. For EU member states where the EIO is not applicable (e.g. Ireland or Denmark), the provisions of Chapter 62a CCP apply within the scope of gathering evidence (Art. 589ka CCP).

The rules of that cooperation are laid down in the CCP. Pursuant to Article 589 w § 1 CCP, when there is a need to obtain or transfer evidence that is located in or may be sent to the territory of another EU member state, known as the ‘executing state’, the court before which the case is being heard, or the prosecutor conducting the investigation proceedings, may issue an EIO, *ex officio* or at the request of a party, defender or attorney, unless the EIO is not applicable in that country.

Article 589g CCP therefore applies together with Chapter 62a CCP, which regulates requests by Polish courts or prosecutors for data located in the territory of another EU member state. Pursuant to Article 589g § 1 CCP, when it is determined that evidence in a case may consist of correspondence, lists of telephone connections or other transfers of information or data stored in an IT system or carrier, including correspondence sent by electronic mail, where these are located in the territory of another EU member state, the court ruling on the case or a prosecutor may send a decision on retaining or securing the data directly to the competent judicial body of that state. After issuing the decision, the authority that issued it submits a motion for the execution thereof directly to the competent judicial body of the EU member state, without the intermediacy of other Polish bodies, particularly the Ministry of Justice. A decision on retaining or securing evidence or securing property (an ‘initial’ decision), therefore, cannot be executed directly in another EU member state.

The application of the provisions of Chapter 62a CCP, including Article 589g CCP, is an exception because they apply only to requests to EU member states to which the EIO does not apply. Instead, the rule is to apply Chapter 62c CCP. Therefore, pursuant to Article 589 w § 2 CCP, where an investigation or screening is being conducted by the police, the Border Guard, the ISA, the National Fiscal Administration, the Central Anticorruption Bureau or the Military Gendarmerie, or where a preparatory proceeding is being conducted by customs and tax authorities as referred to in Articles 133 § 1 and 134 § 1 of the Fiscal Criminal Code, for example by the head of a customs and tax office, the person in charge of the proceedings may also issue an EIO, though this must be approved by a prosecutor before being sent to the foreign state. The provisions state the possibility of an EIO being issued not only after formal initiation of preparatory proceedings but also during the course of screening proceedings as referred to in Article 307 CCP. In court proceedings, the order is issued by the court before which the case is being heard.

⁵⁰ This holds true for all categories of data, even subscriber data.

A decision on issuing an EIO concerning the control and retention of data using technical means of the content of other conversations or transfers of information, including correspondence sent by electronic mail, replaces the decision referred to in Article 237 § 1 CCP (interception and recording of conversations; see Section 14.1.1). The provisions of Chapter 26 CCP apply accordingly (Art. 589 w § 4 CCP). An order, therefore, can only concern the investigation of the crimes described in Article 237 § 3 CCP, and only the persons referred to in Article 237 § 4 CCP. In such a situation, the EIO is sent to the executing state in which the person the EIO concerns is or will be found (Art. 589 w § 6 CCP).

Where operational reconnaissance activities are conducted on the basis of separate provisions,⁵¹ an EIO is issued by the body conducting those activities upon the prior consent of a body of the executing state to the length of the activities and the conditions under which they are to be carried out. For an EIO to be issued, it must be approved by a prosecutor competent on the basis of separate provisions, unless the admission, obtainment or transfer of evidence is reserved for the competent court. Then the issuance of an EIO requires the approval of that court based on separate provisions (Art. 589 w § 7 CCP).

Statistics show that the instrument of the EIO is being used increasingly frequently. In the years 2018–2020, Polish prosecutors sent abroad a total of 17,001 motions concerning the EIO: 3,716 in 2018; 6,702 in 2019; and 6,583 in 2020. That increase concerns the number of EIOs sent from Poland to all EU member states. In the same period, Polish prosecutors received a total of 10,330 motions concerning the EIO from other EU member states: 1,905 in 2018; 4,358 in 2019; and 4,067 in 2020. This data reveals that the overall number of requests sent to Poland from other EU countries was considerably lower than the number of requests from Polish prosecutors to other countries. The increase in EIOs sent from Poland to EU member states is explained by the growing awareness of the usefulness of this instrument among Polish prosecutors and the increase in crime.⁵²

International cooperation on gathering evidence may also take place based on an MLAT. An example of this is the cooperation between Poland and the USA. The two countries concluded an agreement on mutual assistance in criminal cases on 10 July 1996.⁵³ According to this agreement, both parties are to provide mutual assistance in criminal proceedings and crime prevention. The parties shall also provide each other with such assistance in the forfeiture of property and other proceedings directly related to the committing of crimes. The assistance includes, in particular, the delivery of evidence. That agreement is specific in nature, as results from differences between the Polish and American legal systems. The United States is more likely to resort to elements of prosecutorial discretion, unknown in this form in the Polish legal system. In practice, this concerns the American authorities' use of the principles of plea bargaining and probable cause. A public prosecutor in the USA is an active executor of the principle of prosecutorial discretion, and this approach affects legal transactions between the USA and other countries. American prosecutors' use of prosecutorial discretion often leads to

⁵¹ Operational and reconnaissance activities may, for example, be conducted by police on the basis of the provisions of the Act on the Police and aim at checking the previously obtained reliable information about the crime and identifying the perpetrators and obtaining evidence of the crime (Art. 19a paras. 1–2 of the PA).

⁵² J. Klimczak, D. Wzorek and E. Zielińska, *Europejski nakaz dochodzeniowy w praktyce sądowej i prokuratorskiej – ujawnione problemy i perspektywy rozwoju* (Warsaw: Wydawnictwo Instytut Wymiaru Sprawiedliwości, 2022), 100–104.

⁵³ Agreement between the Republic of Poland and the United States of America on mutual legal assistance in criminal matters, done in Washington on 10 July 1996 (*Umowa między Rzeczpospolitą Polską a Stanami Zjednoczonymi Ameryki o wzajemnej pomocy prawnej w sprawach karnych, sporządzona w Waszyngtonie dnia 10 lipca 1996 r.*), Journal of Laws 1999, No. 76, item 860.

a certain type of inertia in implementing requests from Polish parties in cases assessed as insignificant, sometimes referred to as *de minimis* or *low priority*. In such cases, Polish motions are not dealt with for a long time, or the American authorities refuse to deal with them at all, regardless of the fact that the Polish legal system is based on the principle of legalism and that the circumstance of priority does not appear in the Polish–American agreement as a condition constituting grounds for a refusal to implement a request. Another important factor affecting how requests are responded to is the principle of probable cause or justified suspicion laid down in the 4th Amendment to the US Constitution. In accordance with US Supreme Court case law, *probable cause* should be treated as a practical concept allowing a specific compromise to be reached between protecting citizens against unjustified infringement of their basic rights and the need to ensure the performance of lawful police operations. Unfortunately, these differences between the American and Polish legal systems cause practical problems that hamper cooperation. They mainly result from different assessments of the seriousness of a crime, which can result in refusal to provide the assistance requested or in actual abandonment of the activities necessary to provide that assistance. American authorities apply the principle of proportionality, which means prosecuting only in the most serious cases. In cases deemed insignificant, motions for legal assistance are put on the back burner, not dealt with at all or struck off administratively as unfeasible a year after being received. However we assess the attitude of the American authorities, it is necessary to consider that obtaining legal assistance is often obstructed in cases concerning offences that represent a relatively low level of harm to society.⁵⁴

In the absence of an MLA agreement in criminal matters, cooperation takes place on the basis of reciprocity. In practice, this means that a given request may not be carried out by another state.

14.4.2.2 Nature of the Cooperation

Cooperation is of a compulsory character. An EIO should be executed by the body of a state to which a Polish court or prosecutor made a request. Directive 2014/41 foresees, however, that a refusal to execute an order may be issued where a given investigative measure would be inadmissible in a similar domestic case. Furthermore, an executing state may make its consent contingent upon the fulfilment of all the conditions that would apply in a similar domestic case. For this reason, when issuing an order, a Polish authority should bear in mind the competence of the body which is to execute the order regarding the scope of conditions for exercising control over the content.⁵⁵

14.4.2.3 Overview of Existing Cooperation Duties

Within the EU, access to data held by foreign service providers is based on mutual recognition instruments (in particular the EIO). For EU member states where the EIO is not applicable, the provisions of Chapter 62a CCP apply within the scope of gathering evidence. In relation to countries outside of EU, MLATs are used.

Under the procedure of the EIO, an order may be issued for any investigative measure (the scope thereof is not specified in Polish law), provided that this is permissible under Polish

⁵⁴ See P. Radomski, 'Rozdział XIV. Współpraca ze Stanami Zjednoczonymi Ameryki', in J. Gemry (ed.), *Metodyka pracy w sprawach karnych ze stosunków międzynarodowych* (Warsaw: C. H. Beck, 2013), 132, 134–136.

⁵⁵ H. Kuczyńska, 'XII. Nakaz dotyczący kontroli i utrwalania treści rozmów telefonicznych', in J. Skorupka (ed.), *Kodeks postępowania karnego. Komentarz* (Warsaw: Legalis, 2021), n. 41 to Art. 589w.

procedure. Nor does Polish law define the concept of investigative measure, and so one may assume that this encompasses any measure that leads to evidence being obtained.⁵⁶

An order concerning the capture of a telecommunications transmission using the technical means of another member state may be executed in two ways: (1) the telecommunications transmission may be sent immediately to the requesting state or (2) it may be captured and recorded, and only then sent to the requesting state. The issuing authority and the executing authority should consult and agree which method is to be employed. At the moment an order is issued, or even afterwards, during capture, the issuing authority may also – with due cause – request that the recording be transcribed or decoded, with the consent of the executing authority.⁵⁷

Whereas the EIO may be issued for any investigative measure (Art. 589 w CCP), the following decisions are executed under Article 589g CCP: on the seizure of things (Art. 217 CCP), on the seizure of correspondence, lists of telecommunications connections and other information transfers (Art. 218 § 1 and 218a CCP), on the seizure of IT data stored in a system or on carriers, including correspondence sent by electronic mail (Art. 217 § 1 read together with Art. 236a, or Art. 218 § 1 read together with Arts. 236a and 218a CCP).

In practice, the timeliness of an EIO's execution is not always guaranteed, and so it would seem advisable to create mechanisms for monitoring this.⁵⁸ Article 589y CCP lays down the formal requirements for the content of an EIO. Article 589y § 6 CCP provides a basis on which the Minister of Justice may issue, in a regulation, an EIO form template, given the need to provide an executing state with the data it needs to take a proper decision on executing an order. Based on that provision, such a regulation containing a template form for an EIO was issued on 8 February 2018.⁵⁹ A fourteen-page form constitutes an attachment thereto. In practice, this obviously facilitates cooperation, though it should also be pointed out that it is not always necessary to complete the entire form, especially in simple matters, and, furthermore, it is not always necessary to have all of it translated, which is time-consuming and costly.⁶⁰

In connection with the interception and recording of telecommunications ordered with respect to a person staying in the territory of another member state of the EU, if it is not necessary to issue the EIO, the prosecutor or the police notifies a competent authority of the state in point about the intention to carry out said action (Art. 589zd § 1 CCP).

In addition to EU instruments, MLATs may be used for gathering evidence. An example of this is the cooperation between Poland and the USA (see Section 14.4.2.1).

14.4.2.4 Legal Remedies and the Protection of Human Rights

In Polish law there is no possibility of contesting a decision on issuing an EIO, unless a detailed provision on the action called for in the order stipulates otherwise (Art. 589zc § 1 CCP).⁶¹ In Polish legal doctrine, the charge has rightly been made that there is no adequate guarantee in the

⁵⁶ M. Janicz, n. 6 to Art. 589w, in K. Dudka (ed.), *Kodeks postępowania karnego. Komentarz* (Warsaw: Wolters Kluwer, 2018), 1420.

⁵⁷ Kuczyńska, 'XII. Nakaz dotyczący kontroli', n. 39 to Art. 589w.

⁵⁸ Klimczak, Wzorek and Zielińska, 'Europejski nakaz dochodzeniowy', 181.

⁵⁹ Regulation of the Minister of Justice of 8 February 2018 on specifying the specimen form of the European Investigation Order (*rozporządzenie Ministra Sprawiedliwości w sprawie określenia wzoru formularza europejskiego nakazu dochodzeniowego*), Journal of Laws of 2018, item 366.

⁶⁰ Klimczak, Wzorek and Zielińska, 'Europejski nakaz dochodzeniowy', 181–183.

⁶¹ See H. Kuczyńska, 'I. Zaskarżalność', in J. Skorupka (ed.), *Kodeks postępowania karnego. Komentarz* (Warsaw: Legalis, 2021), n. 1 to Art. 589zc.

CCP of an accused person's right to defence, particularly when we consider that, for example, the participation of the defence in the execution of an EIO abroad is severely limited, not only by a lack of appropriate legal regulations but also by practical circumstances. It is rightly argued, then, that this issue should be regulated comprehensively, for example in the form of guidelines that take account of both Directive 2014/41 and the relevant provisions of Directive 2013/48.⁶² Directive 2014/41 provides that its provisions must not violate the right to defence of a person suspected or accused of a crime, or the rights of other persons.⁶³

Pursuant to Article 14 para. 7 sentence 2 of Directive 2014/41, member states should ensure that, when evaluating evidence obtained by means of an EIO, the rights to defence and due process are respected. When assessing the admissibility of evidence, the basic procedural guarantees of the accused must be preserved, particularly those stemming from the European Convention on Human Rights and the Charter of Fundamental Rights. Based on this principle, the courts could apply domestic provisions on the assessment of the admissibility of evidence (e.g. an expert's opinion) less rigorously by invoking the right to defence and due process.⁶⁴ An interested party may demand the application of the procedural guarantees contained in the Directive in the event that these have not been implemented in the law of a given state or were implemented improperly.⁶⁵ A separate issue is the admissibility of evidence obtained through the execution of an EIO issued by a Polish authority, where that evidence is subject to assessment by the Polish courts. Specifically, a problem may arise concerning the use of evidence that was obtained 'by coincidence', meaning the evidence was uncovered in the course of proceedings regarding another (specific) offence and is then used in a different case. A separate procedure should be established to seek the consent of the authority that executed the EIO to the evidence it provided being used in another proceeding.⁶⁶

14.4.3 Cooperation of National Service Providers with Foreign LEAs

Domestic service providers cooperate with foreign LEAs mainly on the basis of the EIO.⁶⁷ Pursuant to Article 589ze § 1 CCP, when an EU member state, known in this context as the 'issuing state', requests the execution of an EIO, a decision in this regard is issued by a prosecutor or court of the district in which the evidence is located or to which it may be transferred. If the admissibility, obtainment or provision of evidence is reserved for the competence of a court or is subject to the order of that court, it is that court that issues the decision (Art. 589ze § 2 CCP). In the case where a court or prosecutor to which an EIO has been addressed is not competent to deal with it, it is sent to the competent court or prosecutor, and notification of this is sent to the relevant court or other authority of the issuing state, known as the 'authority issuing an EIO' (Art. 589ze § 5 CCP). If an EIO was issued by an unauthorised body of the issuing state, it is sent back unexecuted, and the reason for the return is specified (Art. 589ze § 6 CCP).

⁶² Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, [2013] OJ L 294, 6 November 2013.

⁶³ Klimczak, Wzorek and Zielińska, 'Europejski nakaz dochodzeniowy', 191–192.

⁶⁴ H. Kuczyńska, 'XV. Dopuszczalność dowodów uzyskanych w wyniku wydania nakazu dochodzeniowego', in J. Skorupka (ed.), *Kodeks postępowania karnego. Komentarz* (Warsaw: Legalis, 2021), n. 46 to Art. 589w.

⁶⁵ H. Kuczyńska, 'Bezpośrednie stosowanie dyrektywy UE w sprawach karnych. Skutki braku implementacji dyrektywy UE', in D. Czerniak and J. Skorupka (eds.), *Europejskie gwarancje prawidłowego wymiaru sprawiedliwości w sprawach karnych* (Warsaw: C. H. Beck, 2021), 86 *et seq.*

⁶⁶ Klimczak, Wzorek and Zielińska, 'Europejski nakaz dochodzeniowy', 186–187.

⁶⁷ Beyond the EU, MLATs are used for gathering evidence.

A Polish authority (usually a prosecutor's office) that receives an EIO from another country sends a decision on executing the EIO to the relevant company. A decision on executing an EIO concerning the control or retention of the content of telephone conversations, or the recording by technical means of the content of other conversations or information transfers, including correspondence sent by electronic mail, replaces a decision as referred to in Article 237 § 1 CCP. The provisions of Articles 237 § 3-7, 238 § 1 and 2, 239 § 1 and 241 CCP apply as appropriate (Art. 589ze § 10 CCP). Where this concerns the preservation of data, the legal basis is Article 218 CCP. The relevant company then sends a response containing the information requested to the Polish authority that issued the decision. The company cannot refuse to respond to the decision unless the decision fails to meet the formal requirements.

It is not possible to contest a decision to execute an EIO, unless a detailed provision concerning a decision to execute an action identical with that specified in the EIO stipulates otherwise. A challenge may be possible under general rules on the basis of Article 236 § 1 CCP; for example, the way in which an arrest was made or a search conducted could be challenged. In a complaint against an action, the complainant may only demand a verification that the decision on executing the EIO is compliant with Polish law and was executed correctly – if the subject of the complaint is the action itself (Art. 589ze § 7 CCP). The complainant cannot demand that the Polish authority assesses the legitimacy of the control having been ordered – only the issuing state can evaluate the merits of an order, in accordance with the procedures provided in that state.⁶⁸ Further, the Polish authority has an obligation to promptly inform the issuing authority that a complaint was lodged and what the content of its decision in the matter is (Art. 589ze § 8 CCP). Pursuant to Article 14 para. 6 of Directive 2014/41, *the submission of a complaint does not suspend the investigative activity – unless such an effect is foreseen in relation to similar domestic cases.*

If, instead of an EIO, the authority of an EU member state notifies the Polish authority that it intends to intercept, or has intercepted and recorded, telecommunications, the Polish prosecutor subsequently informs this authority whether the thus obtained evidence is admissible in criminal proceedings. This information shall be provided within ninety-six hours of the receipt of the notification by the foreign authority (Art. 589zt CCP). Article 589l CCP regulates the execution by a Polish court or prosecutor of a judgment by a competent judicial body of another EU member state concerning the data preservation in the case of states that do not employ the EIO. Pursuant to Article 589l §§ 1–3 CCP, the geographically competent district court or prosecutor promptly executes a judgment issued by a competent judicial body of another EU member state on retaining potential evidence such as correspondence, shipments, lists of telephone connections or other information or data stored in an IT system or carrier, including correspondence sent by electronic mail, where those things, correspondence, shipments, lists or data are located or stored in the territory of Poland.

As indicated earlier, for EU member states where the EIO is not applicable, the provisions of Chapter 62b CCP apply within the scope of gathering evidence (Art. 589v CCP). In addition to EU instruments, MLATs may be used for gathering evidence.

On the basis of Article 20c para. 8 PA, preserved data (Arts. 180c and 180d TL) and data as referred to in Article 18 paras. 1–5 EPA may also be gathered and made available, upon receipt of a relevant motion, to LEAs of EU member states and other states, to EU agencies involved with preventing and combating crime, and to the International Criminal Police Organization

⁶⁸ H. Kuczyńska, 'VII. Kontrola i utrwalanie treści rozmów telefonicznych', in J. Skorupka (ed.), *Kodeks postępowania karnego. Komentarz* (Warsaw: Legalis, 2021), n. 15 to Art. 589ze.

(Interpol) in order to detect crime and prosecute perpetrators, save human life or health, or search for missing persons.

14.4.4 *Opportunities and Challenges Created by the e-Evidence Regulation*

After five years of difficult negotiations, with sometimes clashing views of the Council of the EU and the European Parliament,⁶⁹ the EU legislator has recently adopted the e-Evidence Regulation.⁷⁰ This Regulation lays down a series of solutions aimed at improving international cooperation in the field of obtaining electronic evidence. It creates a European production order and a European preservation order which require that a member state applies the EU rules to service providers offering services in its territory but based in another member state. Certainly, this new Regulation streamlines the gathering of data in a cross-border context. It eliminates the necessity of filing requests to the competent foreign authorities to request data from the foreign service providers, as it enables direct cooperation with service providers abroad. In Poland, the introduction of these solutions into practice will significantly reduce the waiting period for data, which is currently weeks or more, and thus will accelerate criminal proceedings.

The e-Evidence Regulation also introduces a new data categorisation, with subscriber data and ‘data requested for the sole purpose of identifying the user’ (called ‘access data’ in the European Commission’s initial proposal)⁷¹ on the one hand, and traffic data (previously ‘transactional data’)⁷² and content data on the other. In the case of the former, a public prosecutor or a judge can issue a European production order. In the case of the latter, only a judge can do so. At present, in order to provide subscriber data or access data, no motion or court’s authorisation is necessary because a prosecutor may also request such data. In order to comply with the e-Evidence Regulation by the time it becomes applicable (as of 18 August 2026), it is necessary to introduce into Polish law regulations providing for a mechanism of court authorisation for traffic and content data; in contrast, with respect to subscriber data and traffic data that are only requested to identify a user, an order from a prosecutor will still suffice.

In accordance with the e-Evidence Regulation, if the data required on the basis of a European production order is encrypted, the service provider will not be obliged to decrypt the data.⁷³ In Poland, however, the obligation to decrypt the data content is derived from the general obligations to complete the tasks required by a competent authority (Art. 179 para. 3 TL; see Section 14.1.2.4 of this chapter). Since the authority could not achieve its purpose without decryption, the obliged entity should ensure that decryption takes place. Similar rules should apply when a foreign LEA asks a Polish service provider for data under the procedure of the EIO. Yet, when issuing a European production order in the future, Polish authorities will not be able to require decryption from the addressed foreign service provider.

The e-Evidence Regulation provides for a very limited number of grounds for refusal that the service providers could invoke, which are more reduced than in the Commission’s proposal. These include, for instance, the de facto impossibility of complying with a European production

⁶⁹ For further analysis of the legislative process, see Chapter 7 in this volume.

⁷⁰ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191/118 (e-Evidence Regulation).

⁷¹ Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, [2018] COM/2018/225 final – 2018/0108 (COD), 17 April 2018, Art. 2(8) (Proposed e-Evidence Regulation).

⁷² Proposed e-Evidence Regulation, Art. 2(9).

⁷³ E-Evidence Regulation, Recital 20.

order.⁷⁴ Polish regulations do not provide such ground for refusal, apart from the formal verification of the request. In case the order ‘contains manifest errors or does not contain sufficient information to execute’ it, the service provider should inform the issuing authority ‘without undue delay’ and seek clarification.⁷⁵ Certainly, the latter will allow for a dialogue between the service provider and the issuing authority.

The Regulation also provides for the creation of a European preservation order applicable to all offences and all stored data, but under stricter conditions than Articles 16 and 17 of the Cybercrime Convention (e.g. a time limit of sixty days, which can be extended by an additional thirty days, unless a subsequent request for production is sent, and an obligation for the issuing authority to inform the service provider when preservation is no longer necessary).⁷⁶

Certain elements of the Regulation give cause for concern. For example, the text of the Regulation foresees very short time frames for response (ten days upon receipt of a European production order or within eight hours in emergency cases).⁷⁷ This could be difficult to comply with, particularly for smaller businesses.⁷⁸

14.5 CONCLUSIONS

Due to the international character of services provided and of crimes committed, it is necessary to develop international forms of cooperation that will improve and accelerate crime detection and prosecution. Since the EIO was introduced, it has been used increasingly often as an instrument of international cooperation. Reservations arise as to how the EIO has been implemented in the CCP in Poland. These pertain to an accused person having their right to a defence fully guaranteed, particularly when an EIO is executed abroad. This issue should be regulated through an appropriate amendment of the CCP, or at least through the formulation of guidelines on how the EIO is to be applied, taking account of Directive 2014/41 and the relevant provisions of Directive 2013/48.

The practical application of the EIO to date has shown that the regulations governing it have caused a significant formalisation and unification in international cooperation, which has streamlined cooperation between the authorities of different EU member states. Of particular importance here is having direct contact with the bodies that execute EIOs, for this makes it possible to give further details on what evidence should be collected. Existing practice in the application of the EIO, however, also indicates a need to modify it in certain ways in order to further enhance its effectiveness. These could include addressing delays in execution through the introduction of a mechanism to monitor the progress made by the executing authority. Upon receipt of an EIO, the executing authority would be obliged to send periodic information on what stage of execution has been reached. The issue of evidence obtained under an EIO for the needs of a specific case being used in another case also requires attention, and could be addressed either in the EIO form itself or in a separate procedure where the executing authority grants its consent to the material being used in other proceedings. Consideration should also be given to simplifying the formal requirements in order to improve cooperation. In less complex

⁷⁴ Ibid., Art. 10(7).

⁷⁵ Ibid., Art. 10(6).

⁷⁶ Ibid., Art. 11(1)–(3).

⁷⁷ Ibid., Art. 10(2) and (4).

⁷⁸ M. Rogalski, ‘The European Commission’s e-Evidence Proposal – Critical Remarks and Proposals for Changes, *European Journal of Crime*’ (2020) 28(4) *Criminal Law and Criminal Justice* 333–353.

cases, it is not always necessary to complete the entire form, which contains fourteen pages. The same can be said of having to translate the whole form.⁷⁹

Regarding the Polish domestic provisions, the conceptual framework pertaining to how the terms ‘data’ and ‘electronic evidence’ are used should also be simplified. At present, different concepts are used, and these are spread across several acts (CCP, CC, TL, EPA) and their associated implementing acts. This is not conducive to the efficient practical application of the provisions concerning cooperation between service providers and LEAs.

The law determines when and under what circumstances a service provider is obliged to cooperate with a LEA. Only if there are no legal grounds for the request, or if the grounds are incorrect or unclear, can a service provider refuse to provide data. In practice, such refusals rarely occur. The scope of the reasons for refusal should be wider and include, for example, a manifest violation of a fundamental right.

The data can be retained pursuant to the legal acts regulating the operations of other authorised entities, for example the police. These legal acts provide another mode of supervision. In this scope, a critical view should be taken of the PA, for control over data access is exercised only after the data has been provided, not before. In this sense, the PA may violate the CFREU. In its jurisprudence, the CJEU has pointed to the need to obtain the prior consent of a court or other independent body to data being made available.

The provisions should be amended such that the obligation of providers to cooperate with LEAs is strictly connected with the technical and organisational capacity of a given provider. In practice, the obligation to cooperate with LEAs is very onerous for very small service providers that do not possess appropriate organisational and financial resources.

⁷⁹ Klimczak, Wzorek and Zielińska, ‘Europejski nakaz dochodzeniowy’, 183–187.

Access to Retained Data and Cooperation of Service Providers in Criminal Investigations in Spain

*Carmen Cuadrado Salinas and Juan Carlos Ortiz Pradillo**

15.1 INTRODUCTION

Information and communications technologies (ICT) have had a huge impact on the prevention and investigation of crime. The internet is now the place where evidence must be found, and this permanent and globalised use of technology has forced criminal jurisdictions worldwide to redefine criminal policies and procedures in order to investigate and prosecute crimes using the right tools. In order to do so, legislators have had to redesign the rules required during the criminal investigative stage to address more advanced types of crime and evidence, both related to digital progress. This includes building an innovative legal framework that is more capable and efficient. This framework has provided law enforcement agencies (LEAs) with additional powers, but it has also rebalanced the protection of the fundamental rights involved and created an original one, namely habeas data.¹

Spain entered the new era of investigating cybercrime at a later moment in time compared to other national legislations and, most importantly, compared to European Union (EU) regulations. It was not until nearly the end of 2015 that a new set of rules was established.² Before those legal amendments, LEAs applied very old regulations designed in the nineteenth century and used provisions on searches in physical spaces, which are/were not adapted to searches in cyberspace. Consequently, courts dealt with a large number of cases regarding disputed searches on digital devices, in which the boundaries of the fundamental rights involved were blurred. The

* All translations from Spanish by the authors.

¹ The term habeas data refers to the right to data protection, enshrined in Article 18.4 of the Constitución Española (Spanish Constitution), 29 December 1978, *Boletín Oficial del Estado* (BOE) 29 December 1978, [www.boe.es/eli/es/c/1978/12/27/\(1\)/con](http://www.boe.es/eli/es/c/1978/12/27/(1)/con): ‘The law shall limit the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights.’ (Note to the reader: the *Boletín Oficial del Estado* is the Official Journal of Spain.) In its judgment of 20 April 2016, the Supreme Court expressly forewarned that ‘interferences in the right recognised in Article 18 can be physical or virtual, because the technological revolution offers sophisticated instruments of intrusion that require a functional interpretation of Article 18’. Tribunal Supremo (Spanish Supreme Court), STS 329/2016, 20 April 2016, Fundamento Jurídico (FJ) 2. (Further note to the reader: in Spain, judicial decisions and orders are subdivided not in paragraphs but in so-called *fundamentos jurídicos*. Final judgments are referred to as ‘STS’, followed by the judgment number, while ‘ATS’ refers to orders and ‘STC’ to rulings of the Spanish Constitutional Court.) Furthermore, the Spanish Constitutional Court observed that ‘the advance of current technology and the development of the mass media has forced to extend the protection of the privacy of the family life, home and communications’. Tribunal Constitucional (Spanish Constitutional Court), STC 173/2011, 7 November 2011, FJ 3.

² Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica ((Organic) Law No. 13/2015 on Criminal Procedure in order to strengthen the procedural guarantees and regulate technological investigative measures), 5 October 2015, BOE 6 October 2015. (Note to the reader: ‘organic laws’ are laws that concern fundamental rights, as opposed to ‘ordinary laws’.)

current set of investigative measures completely changed the investigation of cybercrime and one may now argue that Spain has one of the most modern procedures, encompassing the latest high-tech investigative tools and a complete set of cooperation duties for all internet service providers (ISPs). This chapter will describe how Spanish LEAs deal with the search and gathering of electronic evidence and data stored by telecommunications operators and ISPs, according to the new rules which were adopted and as they have been applied by the Spanish courts since the amendments of the Code of Criminal Procedure (CCP) in 2015 and several laws on digital data implemented afterwards in light of relevant EU regulations in the field.

15.2 GATHERING ELECTRONIC DATA IN CRIMINAL INVESTIGATIONS

Sneakers (1992) is an American thriller film about a security specialists team helping National Security Agency (NSA) officers recover a ‘black box’ capable of decrypting any computer system. Talking to Marty Bishop (Robert Redford), Cosmo (Ben Kingsley) says: ‘There is a war out there, old friend, a world war. And it is not about who’s got the most bullets. It’s about who controls the information: ... what we see and hear, how we work, what we think. It’s all about the information.’

In the digital era, information means data. So, the search for information in criminal investigations means the necessity of collecting evidence in digital form, that is, digital data. The Spanish legal reform of the CCP of 2015 updated the domestic framework with a new and modern regulation of technology-related investigative measures that currently allows LEAs to gather electronic data for criminal investigations. The legal reform’s aim was to strengthen the basic procedural guarantees, offering a new and updated legal framework in the field related to new technologies and criminal investigation. Before that, any procedures used in search and seizure of digital devices were governed by outdated rules (from 1882) which only referred to investigative measures used for physical places or spaces rather than cyber spaces. When applying these old procedural rules – set down in Articles 545 CCP and following – courts’ and judges’ decisions were made by extending these rules’ interpretation, which on many occasions meant bending the boundaries established in the Constitution aimed to protect fundamental rights, such as the right to privacy. That atypical situation survived until nearly the end of 2015, when the Spanish legislator decided to amend the investigation stage of the criminal procedure, incorporating new provisions on digital evidence and technology-related investigative measures.

The main reason behind the reform of the CCP³ was to update the Spanish procedural framework, introducing investigatory tools capable of making the investigation of cybercrime more efficient. That was done by a partial reform, necessary to assure compliance with the requirements of the Cybercrime Convention, the European Convention on Human Rights (ECHR) case law and other EU legal instruments.

The current set of investigative measures is by far the most complete and innovative in the field. The measures range from comprehensive interception of telephone and all types of electronic communication to the possibility of using unmanned aerial vehicles (UAVs), Global Positioning System (GPS) tracking devices, international mobile subscriber identity

³ Ley de Enjuiciamiento Criminal (Spanish Code of Criminal Procedure, CCP), Royal Decree 14 September 1882, *Gaceta Oficial*, 17 September 1882, www.boe.es/eli/es/rd/1882/09/14/1/con. The Spanish CCP is so old that the BOE was still named *Gaceta Oficial* or *Gaceta de Madrid* at that time. The *Gaceta Oficial* was the Official Journal used in Spain since 1677, until 1936. In 1936, it was renamed *Boletín Oficial del Estado*. More information at www.boe.es/diario_gazeta/denominaciones.php.

(IMSI) and international mobile equipment identity (IMEI) catchers and base transceiver station (BTS) cell simulators, and also the use of digital undercover agents – police agents acting under an assumed identity in communications held on closed communication channels – as well as remote searches that install tracking software such as a Trojan Horse in order to access the targeted computers. Nevertheless, the new regulations did not include a legal definition or meaning of what should be understood by digital evidence. In broad terms, then, the information obtained in digital format is presented to and assessed by the court as documentary evidence.⁴

As the use of technological measures could interfere with the sphere of basic rights enshrined in various paragraphs of Article 18 of the Constitution (the right to privacy and the secrecy of communications), it was essential to include the obligation of a judicial warrant for investigative measures, such as the use of undercover agents in online communications; capturing or recording oral communications using electronic devices; the use of real-time tracking and location devices (e.g., GPS trackers); searches on mass storage devices; and remote searches on computer systems. This requirement was stressed two years before the reform by the Supreme Court in the judgment of 17 April 2013,⁵ which stated that all information that a person transmits or stores in their electronic devices belongs to what the Court now labels the *right to the virtual environment*.⁶ Since then, the Supreme Court case law has shaped the fundamental right to privacy, giving it a meaning similar to the right of *confidentiality and integrity of information technology systems*.⁷ Furthermore, the Court explained in its later judgment of 4 December 2015 that

beyond the fragmented constitutional treatment of each and every one of the rights that converge . . . , there is a right to the virtual environment itself, integrating, without losing its genuine substantivity, a manifestation of constitutional effect Then, there is a need to provide court protection against the power of the State to invade, in the investigation and punishment of Crimes, that virtual environment.⁸

15.3 DATA RETENTION LEGAL FRAMEWORK

Paraphrasing Asterix's adventures, it could be said that '[t]he year is AD 2022. Data retention on electronic communications and access to retained data by national authorities are governed by the jurisprudence of the Court of Justice of the EU. Well, not entirely . . . One small village of indomitable Spaniards still holds out against the consequences of that jurisprudence.'

The Court of Justice of the European Union's (CJEU) landmark judgment that took place on 8 April 2014, *Digital Rights Ireland* (C-293/12), annulled the Data Retention Directive 2006/24/

⁴ C. Cuadrado Salinas, 'Registro informático y prueba digital: Estudio y análisis comparado de la ciberinvestigación criminal en Europa' (2014) 107 *La Ley Penal* 25–39 at 35.

⁵ STS 342/2013, 17 April 2013, FJ 8.A.

⁶ The content of which, following the Supreme Court ruling, is 'all information in electronic format that, through the use of new technologies, whether consciously or unconsciously, voluntarily or not, is generated by the user, to the point of leaving a trace susceptible of monitoring by the public authorities'. STS 342/2013, 17 April 2013, FJ 8.A.

⁷ In the same sense as it was proclaimed earlier by the German Constitutional Court in its judgment of 27 February 2008. The court ruled that the general right of personality (Art. 2.1 in conjunction with Art. 1.1. of the basic Law (*Grundgesetz*)) encompasses the fundamental right to guarantee the confidentiality and integrity of information technology systems. Bundesverfassungsgericht (German Constitutional Court), 27 February 2008, 1 BvR 370/07, www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2008/02/rs20080227_1bvr037007en.html.

⁸ STS 786/2015, 4 December 2015, FJ 1.F.

EC⁹ and caused an endless landslide¹⁰ of legislative reforms in some EU member states. Unlike other constitutional courts that reformed their national laws due to the invalidated Data Retention Directive (e.g., Belgium, France and Germany), the Spanish courts considered that Law No. 25/2007 generally complied with the requirements established in *Digital Rights Ireland* in terms of the levels of security that should be applied to data retention; the existence of an authority of supervision, such as the Spanish Agency for Data Protection; the need for a judicial decision to gain access to retained data; and the submission of that access to the principles of specialty, suitability, exceptionality and necessity. In other words, retained data may be used in criminal proceedings for the investigation and prosecution of serious crimes only with a prior judicial authorisation, and that order must be reasoned. That is why the Spanish legislation on data retention is still regulated in the same Law No. 25/2007¹¹ on the Retention of Data Relating to Electronic Communications and to Public Communication Networks, enacted precisely in order to comply with the annulled Directive 2006/24/EC.

Since the *Digital Rights* Case, the CJEU has established a quite detailed case law referring to the retention of electronic communications data and its use for the prevention, investigation, detection and prosecution of criminal offences (among others, see its judgments in *Telez Sverige/Watson* (Joined Cases C-203/15 and C-698/15), *Ministerio Fiscal* (Case C-207/16), *Quadrature du Net* (Case C-623/17 and Joined Cases C-511/18, C-512/18 and C-520/18) and *Garda Síochána* (Case C-140/20)), which results, as we already indicated, in the Spanish national regime not being compatible either with the EU Directives or the Charter of Fundamental Rights of the European Union.¹²

The Spanish jurisprudence focuses all its attention in highlighting the high level of protection of the retained data and the specific requirements and safeguards included in order to obtain access to the retained data. It is true that the new regime governed under the CCP 2015 has introduced proper safeguards and individual rights in favour of the investigated person and that access to and use of those stored data are now subject to a duly reasoned and weighted judicial decision. But the Spanish courts forget the original sin of our system: the disproportionate and indiscriminate retention regime contained in Law No. 25/2007.

The latest CJEU jurisprudence has pointed out that the retention itself constitutes an interference with the fundamental rights of privacy and protection of personal data. And there has been no progress in the Spanish legislation to comply with the CJEU case law referring to the retention system. Although the legislation governing access to retained data has been subject to the proportionality principle since 2015, the retention and storage obligations in Law No. 25/2007 must be qualified as a general and indiscriminate data retention regime that constitutes an unjustified serious interference with the rights to privacy and data protection. For instance, the retention period for all categories of data still continues to be a general period of twelve months! Nevertheless, the Supreme Court has always proclaimed that the regime of retention *and* access

⁹ Directive 2006/24/EC of the European Parliament and of the Council of 15th March 2006 on the retention of data generated or processed in connection with the provisions of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 2006 OJ L 105, 13 April 2006.

¹⁰ Jones Day, 'The Data Retention Saga Continues: European Court of Justice and EU Member States Scrutinize National Data Retention Laws', Lexology, 11 August 2016, www.lexology.com/library/detail.aspx?g=a886514b-71ab-4779-a2e7-d1486076e01b.

¹¹ Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (Law No. 25/2007 on the Retention of Data Related to Electronic Communications and Public Communications Networks), 18 October 2007, BOE 19 October 2007, www.boe.es/eli/es/l/2007/10/18/25/con.

¹² See J. C. Ortiz Pradillo, 'Europa: auge y caída de las investigaciones penales basadas en la conservación de datos de comunicaciones electrónicas' (2020) 52 *Revista General de Derecho Procesal* 1–42.

to data, stored under the legal framework of Law No. 25/2007, must be read in conjunction with the CCP, which governs the access of public authorities to such data.

Furthermore, Law No. 25/2007 introduced an amendment to the Law of General Telecommunications,¹³ establishing that service providers operating public communication networks or providing available electronic communications services should ensure the secrecy of communications, but are also obliged to carry out the intercepts that are authorised within the criminal procedure. In that sense, the obliged entities must provide to the authorised agent the data indicated in the order of interception;¹⁴ the exception is when, due to the characteristics of the service, it is not at their disposal. The Law states that the identity or identities of the subject of the interception measure must be recorded;¹⁵ the location of the terminal or termination point network origin of the call; and the target of the call.¹⁶ In the case of mobile services, an accurate position of the point of communication must be provided as well as the identification, location and type of station base affected.

Although the Spanish case law considered that Law No. 25/2007 (Data Retention Law) generally did comply with the requirements established in *Digital Rights Ireland*, it underwent some important modifications after the invalidation of the Data Retention Directive, which were provided for in the reform of the General Telecommunications Law of 9 May 2014,¹⁷ and by the above-mentioned reform of the CCP of 2015.

The latter reform, however, failed to resolve an important point that had been controversial for some time: the definition of ‘serious crime’, which is the threshold justifying access to data. In the substantive law, serious crime is defined in Articles 13 and 33 of the Criminal Code. The first one rules that serious crimes are ‘offences that the Law punishes with serious penalties’ and the second one establishes as a serious penalty, among others, imprisonment exceeding five years. However, that definition does not apply in criminal procedure. The procedural criteria to allow investigative measures that constitute an interference with fundamental rights (and the access of public authorities to such retained data constitutes an interference with the fundamental right to respect for private life, enshrined in Article 7 of the Charter) are not only based on the seriousness of the offence.

The Supreme Court and the Constitutional Court have stated that the seriousness of the offence should not be determined exclusively by the years of imprisonment only, but rather by other criteria such as the protected right, the social impact of the crime or there being a criminal

¹³ Ley General 32/2003 de Telecomunicaciones (General Telecommunications Law No. 32/2003), 3 November 2003, BOE 4 November 2003, Art. 33.

¹⁴ The amended Article 33 of General Telecommunications Law No. 32/2003 states that the operators are obliged to carry out the seizure and recording of the content of communications with an indication of the manner or type of communications affected, and any other type of data indicated in the order of legal interception, for example: knowledge of its origin or destination, at the time the communication is made; the identity or identities of the other parties involved in the electronic communication; the geographic location of the origin or destination of the communication; any basic or additional services used; the address of the communication; the response indication; the cause of completion; and location information or any information exchanged through the control or signalling channel.

¹⁵ ‘Identity’ is defined as a technical label that can represent the origin or destination of any electronic communications traffic, in general identified by a physical electronic communications identity number (such as a telephone number) or a logical or virtual electronic communications identity code (such as a personal number) that the subscriber can assign to a physical access on a case-by-case basis.

¹⁶ For instance, the identity or identities of the other parties involved in the electronic communication; the basic services used; the supplementary services used; the address of the communication; the response indication; the cause of termination; any temporary marks; the location information; and the information exchanged through the control or signalling channel.

¹⁷ General Telecommunications Law No. 32/2003 was replaced by General Telecommunications Law No. 9/2014, BOE 10 May 2014, www.boe.es/eli/es/l/2014/05/09/9/con. And this one was replaced by General Telecommunications Law No. 11/2022, 28 June 2022, BOE 29 June 2022, www.boe.es/buscar/doc.php?id=BOE-A-2022-10757.

organisation involved.¹⁸ Moreover, the Constitutional Court judgment of 3 April 2006¹⁹ stated that the incidence of the use of digital data, both for the perpetration of the crime and for perverting the course of justice, could be a valid criterion in order to determine that this is indeed a serious crime, legitimising the use of any legal tool aimed at limiting the fundamental right of secrecy of communications, and hence justifying the use of ICT investigative measures.

These case law-based criteria were expressly introduced in the legal reform of the CCP in 2015. After the amendments of the CCP of 2015, use of the new investigative measures²⁰ is limited to situations where the following criteria are fulfilled: (i) the situation is of an exceptional nature and particular necessity; (ii) when the investigation cannot be otherwise carried out due to the impracticability of any other measures available and less invasive to fundamental rights, but equally useful for clarifying the facts; or (iii) when the evidence gathered, the verification of the perpetrators or the location of the effects of the crime could be seriously undermined, if that specific measure has not been used.

Furthermore, the CJEU, in *Ministerio Fiscal*, confirmed that the reasoning of the Spanish government and the Spanish Public Prosecutor in relation to the proportionality of the interference was correct because the amendment of the CCP in 2015 introduced new alternative criteria to allow investigative measures that constitute an interference with fundamental rights (e.g., the access of public authorities to such retained data is considered an interference with the fundamental rights of Arts. 7 and 8 of the European Charter). Those criteria assess the proportionality of the investigative measure according to the seriousness of the interference in the privacy and not only according to the penalty attached to the crime investigated. For the Spanish government, when the interference that such access entails is not serious, it may be justified by the objective of preventing, investigating, detecting and prosecuting ‘crimes in general’. The Spanish Public Prosecutor concluded that accessing data for the sole purpose of identifying the holders of subscriber identity module (SIM) cards activated for a period of twelve days with the IMEI number of the stolen mobile phone should not be considered, in that light, a ‘serious’ interference.²¹ The CJEU confirmed that reasoning expressly when it said:

In accordance with the principle of proportionality, serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as ‘serious’.

By contrast, when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting ‘criminal offences’ generally.²²

In other words, the Spanish government reasoned that asking for subscriber data for the sole purpose of identifying users (such as personal data relating to the identity of the owners of SIM cards) should not be considered ‘serious’ interference, so it may be done for criminal offences generally, unlike access to traffic or location data, which is considered a serious interference and thus can be used only in investigation of serious crimes.²³

¹⁸ STC 184/2003, 23 October 2003, FJ 1.

¹⁹ STC 104/2006, 3 April 2006, FJ 3.

²⁰ Such as the interception of telephone and all types of electronic communications, e.g., the possibility of using unmanned aerial vehicles (UAVs), GPS tracking devices, IMSI-IMEI catchers and BTS cell simulators, digital undercover agents, remote searches, and installing a tracking device such as a Trojan Horse software to access the targeted computers.

²¹ Case C-207/16, *Ministerio Fiscal* [2018] ECLI:EU:C:2018:788, paras. 53–59.

²² *Ibid.*, paras. 56 and 57.

²³ Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net* [2020] ECLI:EU:C:2020:791, para. 117. See also *La Quadrature du Net*, para. 140:

15.3.1 *The Guiding Principle: Necessity of a Judicial Warrant*

As a general rule, the use of any of the technology-related measures needs prior judicial authorisation. Unlike other national legal frameworks, those operations that would directly affect the fundamental right to privacy and the secrecy of communications cannot be authorised by an administrative authority; they must be authorised by a court. Even access to retained data by LEAs and other competent national authorities (for instance, custom agents are also considered police in Spain) is subject to prior authorisation by a criminal court. In Section 15.3 we explained that the Spanish regime of access to retained data is subject to a duly reasoned and weighted judicial decision.

That aside, the principle of necessity of a judicial warrant introduced by the CCP 2015 (with some specific exceptions in cases of urgency²⁴) leads to the need of a clear and very individualised motivation for the warrant. The judicial decision authorising the investigative measure must specify, as a minimum, the following facts: the punishable act subject to investigation and its judicial classification, with a statement of the *prima facie* evidence grounding the measure; the extent of the interception measure, specifying its scope, duration and the grounds that justify the necessity and the proportionality of the measure; and the identity of those under investigation and any other third person affected by the measure, if known. Pursuant to this aspect, investigative measures may be ordered even when they affect third parties (e.g., when the terminals or means of communication subject to intervention are property of third persons but are habitually or occasionally used by the person under investigation, or when it is necessary to intercept the victim's terminals or means of communication where a serious risk to their life or integrity is foreseeable).²⁵

On the other hand, there is a substantial difference between the phase of seizure of the electronic device and the phase of access to its content. It is considered that the seizure of such devices does not legitimise access to their content; this requires further judicial authorisation, which may be granted either in the warrant for seizure or in a later decision.²⁶ Finally, when examining the validity and the authenticity of the evidence provided by the courts, judges place special emphasis on expert examination of the devices and electronic evidence to verify that they were not altered.²⁷

15.3.2 *Categorisations of Data and Constitutional Rights Affected*

15.3.2.1 A Brief Introduction to the Difference between the Right to Privacy and the Right of Secrecy of Communications Protected by Article 18 of the Constitution

Generally speaking, the need for a judicial order depends on the fundamental right affected, distinguishing if the affected right is the fundamental right to privacy enshrined in Article 18.1 of

As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, in accordance with the principle of proportionality, only action to fight serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter ... Accordingly, only non-serious interference with those fundamental rights may be justified by the objective of preventing, investigating, detecting and prosecuting criminal offences in general (see to that effect, C-203/15 and C-698/15, *Tele2* [2016] ECLI:EU:C:2016:970, para. 102, and *Ministerio Fiscal*, paras. 56 and 57; Opinion 1/15, *EU–Canada PNR Agreement*, [2017] ECLI:EU:C:2017:592, para. 149).

²⁴ Art. 588 ter d (3) CCP establishes that, in cases of urgency related to terrorism crimes and organised criminal networks, the Home Office is allowed to issue a valid order instead of a judicial warrant. However, the content of that order must be sent to the judge immediately, and the judge in a maximum period of twenty-four hours should confirm or deny that order.

²⁵ Art. 588 ter b (2) CCP.

²⁶ Arts. 588 sexies b and 588 sexies c CCP.

²⁷ E. Velasco Nuñez, *Delitos cometidos a través de internet* (Madrid: La Ley Temas, 2010), 251.

the Constitution or the right of secrecy of postal and telephone communication established in Article 18.3. Regarding the content of the latter, the concept of secrecy is purely a formal requirement,²⁸ in the sense that what is protected is only the *process of the communication*.²⁹ What the Constitution guarantees then is the ‘secrecy of the communication’ by banning the use of illegal devices with the aim of allowing a third person to interfere into the communication between the transmitter and the receiver. In that sense, it is an offence against that fundamental right to use any illegal device, such as telephone tapping, listening devices, surveillance devices or any other equipment or tool capable of intercepting an ongoing communication. On the other hand, the scope of protection provided by Article 18.1 relates to the content of the communication, which is the information that could affect the privacy of any of the parts of this communication. In that sense, the doctrine of the Constitutional Court clearly states that the protection of the right of secrecy of communications is maintained during the time the communication is ongoing, but when the communication terminates, the constitutional protection ceases. Thus, the right to privacy may or may not be affected, even when there has been a breach of Article 18.3.³⁰ Consequently, whereas the interception of communication always requires a judicial order, the right to privacy does not demand this requirement in every single situation.³¹ In saying that, the Constitutional Court is recognising that in certain cases in which the right to privacy is involved, LEAs do not need a judicial warrant. Examples are when police searches have reasonable grounds to suspect that a person is carrying illegal drugs or any other illegal item; or when searching a vehicle.³²

15.3.2.2 Content Data and Non-content Data

In relation to digital devices, as a means to define their scope and the safeguards and requirements when LEAs are carrying out a search and seizure of such devices, the traditional distinction has been applied between *content data* and *non-content data*. Non-content data is protected by the fundamental right of secrecy of communications (Article 18.3 Constitution) and refers to the process of communication itself, that is, from the formal point of view explained in Section 15.3.2.1. Content data, however, relates to the information contained in the proper digital device, and in that sense it is protected by the right to privacy (Article 18.1 Constitution), which does not always require a judicial order. Nevertheless, for the purpose of assessing the seriousness of the interference into the privacy sphere, Spanish case law has considered that in that field, the doctrine of the *reasonable expectation of privacy*³³ should be applied as a theoretical tool in order

²⁸ STC 70/2002, 3 April 2002, FJ 9.3.

²⁹ STC 170/2013, 7 October 2013, FJ 4.a.

³⁰ STC 123/2002, 20 May 2002, FJ 4.

³¹ STC 70/2002, 3 April 2002, FJ 10 b.3.

³² See J. C. Ortiz Pradillo, *Problemas procesales de la ciberdelincuencia* (Madrid: Colex, 2013), 189.

³³ In following the case law of the ECHR in the case *P.G. and J.H.*, Appl. No. 44787/98, 25 September 2001, para. 57:

There are a number of elements relevant to a consideration of whether a person's private life is concerned in measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain.

to make a decision of whether the information obtained by the police without any judicial order was legally or illegally obtained.

For example, in relation to the seizure of mobile phones, the Supreme Court judgment of 25 September 2003 stated that LEAs could investigate the phone numbers recorded in the memory of the mobile devices without seeking a judicial authorisation ‘because that electronic telephone book is equated with any other physical telephone book in which the holder can save numbers of telephones and annotations’.³⁴ When accessing the internal memory of a mobile phone or computer system, it was traditionally understood that any matter not referred to the process of communication should be placed within the sphere of the right to privacy (Article 18.1 Constitution). As explained in Section 15.3.2.1, the Constitutional Court stated that there was no obligation for prior judicial warrants when the privacy of a person was at stake. Therefore, the police were allowed to gain access to that information when the interference of the right to privacy was not considered serious and when there was urgency and necessity to carry out the investigative measures in question. This doctrine was fortunately abandoned after the Constitutional Court judgment of 5 November 2007,³⁵ in which the Court stated that access to a mobile phone is contrary to Article 18.3, and therefore a judicial authorisation is needed. However, the Constitutional Court stated in a judgment of 14 March 2011 that obtaining the telephone number and the name of the owner is a non-serious infraction of Article 18.1, so access to that data was substantiated because it was a suitable means to achieve a legitimate aim.³⁶

Two years later, the Constitutional Court declared in its judgment 115/2013³⁷ that a new approach regarding cases including digital evidence was necessary and thus recognised the impact that technological development entails in the way LEAs act in criminal proceedings, and in the proper protection of the fundamental rights affected. In doing that, the Constitutional Court anticipated the new approach declared in the famous US Supreme Court landmark case *Riley v. California* (2014) more than a year later, in which Judge Alito declared that ‘we should not mechanically apply the rule used in the predigital era to the search of a cell phone. Many cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form. This calls for a new balancing of law enforcement and privacy interests.’³⁸

According to this new approach, the reformed CCP of 2015 came up with the obligation for LEAs to obtain a judicial warrant prior to accessing the memory of an electronic device such as a computer, telephone or any other online communication instrument or mass digital information storage device. More specifically, to be able to understand to what extent the basic rights enshrined by the Constitution are protected, it should be mentioned that the right of secrecy of communications (Article 18.3) is still conceived as a right ‘of formal content’ as explained in Section 15.3.2.1 (protecting only the process of the communication, regardless of the type of information concerned).³⁹ Notwithstanding that conception, it is understood now that the meaning of *secrecy of communication* covers not only its formal content (i.e., the process) but also other aspects of the communication such as the telephone number of the person making the communication, and of the individual who receives it, along with other external data related to the communication such as its time, duration and destination. In conclusion, and as a rule, the

³⁴ STS 1231/2003, 25 September 2003, FJ 8.

³⁵ STC 230/2007, 5 November 2007, FJ 2.

³⁶ STC 25/2011, 14 March 2011, FJ 5.

³⁷ STC 115/2013, 9 May 2013, FJ 4.

³⁸ *Riley v. California*, 573 US (2014). Opinion of Alito, J. at point B.

³⁹ As the ECHR warned in *Malone v. The United Kingdom*, Appl. No. 8691/796, 2 August 1984.

traffic data that has been originated in connection with a process of communication is also protected under the umbrella of the secrecy of communication (Article 18.3 Constitution).

When dealing with cases of drafted emails, it was understood by the courts that since no sending activity had been produced, no process of communication existed; therefore, it could not be covered by the right of secrecy of Article 18.3. However, after the reform of CCP in 2015, the rule is that the search of a computer system – whether it occurs due to a search and seizure at a home or outside – must require a judicial warrant. Therefore, if these draft emails are located on a personal computer (PC) that is being seized, a specific judicial warrant must be obtained to examine the internal memory of the device containing those draft emails. In other words, drafted emails are considered content data, similarly to chat rooms and communication in the context of online games.

15.3.2.3 Static Data and Dynamic Data

As explained in Section 15.3.2.1, during the last five years the jurisprudence has shifted towards a progressive abandonment of the *formal* protection of Article 18.3 of the Constitution in relation to the right of secrecy of communication. The new interpretation regarding the right protected by Article 18.3 was triggered by the judicial recognition of a *reasonable expectation of privacy* for both transmitter and receiver. Therefore, there is now a more solid jurisprudence according to which some *external data of an electronic communication* should be covered not by the Malone doctrine⁴⁰ but rather by the rules on personal data associated with a communication process that does not identify the communicants.⁴¹ In that sense, the recent Supreme Court's case law has clearly identified the need to differentiate between a *static concept of data* and a *dynamic concept of data*.

The static concept of data refers to the data generated when the communication has ended and, as a result of that, that kind of data is stored, conserved or treated by service providers; consequently, it is data no longer related to the process of the communication because that process has ended. In contrast, the *dynamic concept of data* refers to the *external or traffic data*. In other words, it is the data obtained while the process of the communication is ongoing, which is then capable of revealing all or part of the information related to the process of the communication protected by Article 18.3 of the Constitution (secrecy of communication). That new perspective in relation to the right of secrecy of communication led the Supreme Court to further define *traffic data* as the external data of any specific communication, and therefore incorporated within the protective umbrella of Article 18.3, in comparison with any other information that is not personal data but travels along with the communication made, and therefore is associated with it in an accessory way to the communication process.

To summarise, the Supreme Court distinguishes between (a) external personal data or traffic data when it is referring to a specific communication and the data is capable of revealing all or part of the secrecy that is protected by Article 18.3 of the Constitution, and (b) the circumstances

⁴⁰ In the sense of the content of *Malone v. The United Kingdom*, para. 56:

[T]he process known as 'metering' involves the use of a device called a meter check printer which registers the numbers dialled on a particular telephone and the time and duration of each call. It is a process which was designed by the Post Office for its own purposes as the corporation responsible for the provision of telephone services. Those purposes include ensuring that the subscriber is correctly charged, investigating complaints of poor-quality service and checking possible abuse of the telephone service. When 'metering' a telephone, the Post Office – now British Telecommunications – makes use only of signals sent to itself.

⁴¹ STS 4084/2017, 16 November 2017, FJ 2.

or personal data related to privacy, protected by Article 18.1, but disconnected from the communication process that is protected by Article 18.4 of the Constitution (right to habeas data).⁴² Pursuant to Article 588 ter CCP 2015, traffic data is now considered as electronic data or associated traffic data, and refers to all data generated as a result of the communication transmission through a network of electronic communication, making it available to the user, as well as the provisions of an information society service or telematic communication of analogous nature.⁴³

Some of the examples attached to the case law evolution refer to access by police to IMSI and IMEI numbers, using cell site simulators. These IMSI and IMEI numbers are considered personal data because each, despite being an alphanumeric key that by itself does not reveal anything but a succession of numbers, could be completed with other data, which is usually in the possession of the telephone service operator, and converted into data which is capable of identifying any person or legal entity.⁴⁴ In this case, it is understood that the IMSI, by itself, is neither data that could be part of the legal concept of ‘communication’ nor data that could be framed in the sphere of the constitutionally protected right of habeas data (Article 18.4). On the other hand, the IMSI needs to be merged with other data which is in the possession of the service provider in order to be considered data protected by Article 18.4. Consequently, access by LEAs to the IMSI, through transfer of data by the telephone service provider, needs a judicial warrant.

This is, according to the new CCP 2015 regulations (i.e., Articles 588 ter (l) and (m)), the rule whereby LEAs may use technical devices capable of allowing them to find out the identification codes, technical labels, telecommunications devices or any of their components, such as IMSI or IMEI numbers. Once the codes allowing identification of the device, or any of its components, have been obtained, LEAs must seek judicial authorisation in order to obtain any personal data available (subscriber’s data) from the service providers.

In relation to internet protocol (IP) addresses as data obtained by LEAs, there has also been a progressive consideration. Initially the IP address was conceived as traffic data, but now it is conceived as personal data.⁴⁵

In relation to the concept of *personal data*, the General Data Protection Regulation (GDPR) is also of application. It was implemented in Spain under (Organic) Law No. 3/2018 of 5 December 2018 on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD),⁴⁶ which has recognised a new set of digital rights for citizens that forms part of

⁴² STS 247/2010, 18 March 2010, FJ 3.3.

⁴³ A similar definition is provided for in Art. 64 of the Real Decreto 424/2005 por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios (Royal Decree No. 424/2005 on the conditions for the provision of electronic communications services, universal service and users protection), 15 April 2005, BOE 29 April 2005, www.boe.es/buscar/act.php?id=BOE-A-2005-6970.

⁴⁴ STS 249/2008, 20 May 2008, FJ 4.D.

⁴⁵ Even if data protection and privacy are fundamental rights,

[p]ersonal data and private data are not synonymous. Personal data are any kind of information (alphanumeric, graphic, photographic, acoustic, etc.) concerning an identified or identifiable natural person, irrespective of whether this information is private. However, data regarding ideology, trade union membership, religion, beliefs, racial origin, health or sex life as well as criminal and administrative offences are deemed more sensitive and require specific protection. (L. López-Lapuente and R. Bermejo Bosch, ‘Spain’, in Alan Charles Raul (ed.), *The Privacy, Data Protection and Cybersecurity Law Review*, 5th ed. (London: Law Business Research, 2018), 306, www.uria.com/documentos/colaboraciones/2319/documento/Spain_rbb.pdf?id=8293_en)

⁴⁶ Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales ((Organic) Law No. 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights), 5 December 2018, BOE 6 December 2018, www.boe.es/eli/es/lo/2018/12/05/3.

the content of Article 18.4 of the Constitution.⁴⁷ This is stated in Article 1 of the LOPDGDD, where it is established that the protection of any person in relation to personal data is a fundamental right enshrined in Article 18.4 of the Constitution and, as such, is included in the right to habeas data.

However, the concept of ‘personal data’ is defined under an even earlier data protection law: (Organic) Law No. 15/1999 on the Protection of Personal Data (LOPD).⁴⁸ According to Article 3 LOPD, personal data is *any information concerning identified or identifiable persons*.

Moreover, personal data processing and collection in the field of criminal investigations is governed by two essential laws: Law No. 25/2007 of 18 October 2007 on the Retention of Data Related to Electronic Communications and Public Communications Networks and (Organic) Law No. 7/2021 on the Protection of Personal Data Processing for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,⁴⁹ which was adopted to comply with Law Enforcement Directive (LED) (EU) 2016/680. Article 3 of (Organic) Law No. 7/2021 reproduces the content of Article 3 of the LED and Article 5 of Law No. 25/2007 reproduces the content of Article 5 of the Data Retention Directive.

However, the initial consideration of the term ‘personal data’ given by Article 22.2 LOPD, according to the interpretation of the Spanish Agency for Data Protection,⁵⁰ allowed LEAs to obtain an IP address when that information was necessary to prevent a real danger to public safety or as evidentiary information in criminal procedures.⁵¹ In similar terms (although the Council of Europe initially considered the IP address as traffic data able to identify the *origin* of a communication), the Committee of the Convention against Cybercrime (T-CY)⁵² declared that the definition of *traffic data* contained in Article 1(d) of the Convention was too broad, and the IP address used in a specific communication when it has already ended should be regarded as *data relating to the subscriber*. More particularly, it should be included within the expression

⁴⁷ For instance, the right to internet neutrality (as the right to obtain from the internet services providers a transparent service offer without discrimination for technical or economic reasons); the right to universal access to the internet (as the right to access a universal, affordable, solid and non-discriminatory service for the entire community); the right to digital security (of their communications through the internet); the right to digital education; protection of children on the internet (public prosecutors shall intervene in those cases of unlawful intrusion by means of the use or disclosure of images or personal information concerning children on social media or information society services); the right to rectification in the internet (such as the right to freedom of speech on the internet. The social media, digital platforms and information society services managers or controllers shall adopt protocols for exercising the right to rectification of the content which violates any person’s right to honour, personal or family privacy or to communicate or receive truthful information); the right to the update of information in digital communication media; the right to privacy and use of digital devices in the workplace (as the right to privacy in relation to digital devices at the employee’s disposal); the right to digital disconnection in the workplace; the right to privacy related to the use of video surveillance and sound recording devices in the workplace; digital rights in collective bargaining; and so on.

⁴⁸ Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal ((Organic) Law No. 15/1999 on the Protection of Personal Data), 13 December 1999, BOE 14 December 1999, www.boe.es/eli/es/lo/1999/12/13/15/con.

⁴⁹ Ley Orgánica 7/2021 de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales ((Organic) Law No. 7/2021 on the Protection of Personal Data Processing for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties), 26 May 2021, BOE 27 May 2021, www.boe.es/eli/es/lo/2021/05/26/7/con.

⁵⁰ Agencia Española de Protección de Datos (Spanish Agency of Data Protection), Report 327/2003 on the personal data nature of the IP address (Madrid: AEPD, 2003), p. 2, www.aepd.es/es/documento/2003-0327.pdf.

⁵¹ Agencia Española de Protección de Datos (Spanish Agency of Data Protection), *Annual Report 2004* (Madrid: AEPD, 2004), p. 121, www.aepd.es/es/documento/memoria-aepd-2004.pdf.

⁵² Council of Europe, T-CY Guidance Note #8: *Obtaining Subscriber Information for an IP Address Used in a Specific Communication within a Criminal Investigation*, 12 November 2013, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7130>.

any other access number mentioned in Article 18 (3) of the Convention, regardless of whether it is a static IP address permanently assigned to a single user or a dynamic address assignable successively to multiple users, in accordance with what was previously explained in sections 179 and 180 of the Explanatory Report to the Cybercrime Convention.

In sum, the Spanish case law concluded that the IP address, like the IMSI and IMEI algorithms, was nothing more than a numerical label that did not identify the user or subscriber by itself; therefore, it was understood that once it was introduced by its owner to the internet, no judicial warrant was needed to get what was already public.⁵³ However, once the IP is known by the police, the subsequent identification and location of whoever is assigned that IP must be carried out under judicial control.⁵⁴

Finally, the doctrine of the Supreme Court in relation to evidence gathered without judicial warrant of an IP address used in an ended communication and through a peer-to-peer (P2P) network combines two important arguments. On the one hand, it applies the static concept of data as the information is stored after the communication has ended. On the other hand, it applies the dynamic concept according to which the interception of an IP address, while the connection is on and through the internet, should be understood as a key in facilitating the routing of the communication, and then it would require a judicial warrant for the information to be legally gathered.

With the same meaning, the above-mentioned Proposal of the Committee of the Convention against Cybercrime (T-CY) from 12 November 2013 recognises that the IP address could be considered as traffic data when, for example, it is intercepted along with other traffic data or the contents of a real-time communication. And, on the other hand, the consideration that the information has been made public by the user (in absence of a real expectation of privacy or presumed consent) resembles the doctrine of the US Supreme Court that holds that internet users do not have a legitimate expectation of privacy with respect to all email addresses, the IP addresses of the websites visited, the total volume of user traffic and other routing information transmitted to third parties (the ISPs) for the purposes of the transmission of internet communications.⁵⁵

15.4 SERVICE PROVIDERS AND THE SPANISH LAW: AN INTRODUCTION TO THE COOPERATION DUTIES

In the past, Spanish law differentiated between ISPs and telephone service providers. The former were regulated by Law No. 34/2002 on Information Society Services and Electronic Commerce (amended by Law No. 15/2022 of 12 July),⁵⁶ whereas the latter were subjected to the obligation of data retention established in Law No. 25/2007.

⁵³ For further information about the former Spanish regulation, jurisprudence and a comparative study of the English regulation on cybercrime, see Cuadrado Salinas, 'Registro informático', 25–39.

⁵⁴ J. M. Sánchez Siscart, 'A vueltas con el secreto de las comunicaciones: algunos supuestos críticos en la jurisprudencia de la Sala 2.ª del Tribunal Supremo' (2010) 7338 *Diario La Ley* 20.

⁵⁵ Compare with *United States v. Forrester*, 512 F. 3d 500, 510 (9th Cir. 2008), as well as *Smith v. Maryland*, 442 EE.UU. 735, 743–744 (1979): 'Computer users have no legitimate expectation of privacy in dialing, routing, addressing, and signaling information transmitted to telephone companies. . . . E-mail addresses and IP addresses provide addressing and routing information to an Internet service provider (ISP) in the same manner as a telephone number provides switching information to a telephone company' (*United States v. Forrester*, 510).

⁵⁶ Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico (Law No. 34/2002 on Information Society Services and Electronic Commerce, amended by Law No. 15/2022) 11 July 2002, BOE 12 July 2002, www.boe.es/buscar/act.php?id=BOE-A-2002-13758.

During the development of the new regulations set down by the CCP 2015, a problem arose with some companies acting as communications operators but not specifically as *providers of internet access* (e.g., Vodafone, Movistar); accordingly, the obligation of data retention established in Law No. 25/2007 did not apply to them. In relation to the provisions of CCP 2015, the new Article 588 ter (e) clearly states that the law applies to all providers and that they all have a legal duty to cooperate with the authorities. The obligation to cooperate applies not only to ISPs but to all providers of telecommunications and information society services, as well as any other person who could contribute to facilitating communications. In all those cases, the information could be retained ‘in compliance with the legislation on data retention relating to electronic communications [i.e., in compliance with Law No. 25/2007], or on their own initiative for commercial or other reasons linked to a communication processes’, such as for billing purposes (e.g., downloaded apps) or for other added-value services (e.g., geolocation services).⁵⁷ Under both regimes, the police must seek judicial authorisation to obtain traffic or location data.

In general, the CCP 2015 establishes the obligation of third parties to cooperate with criminal investigations, the nature and content of which, however, would depend on the specific technological investigation measures used by LEAs. The CCP 2015 provides for different measures: the interception of telephone and electronic communications; the use of technical devices for surveillance and real-time geolocation (e.g., using GPS);⁵⁸ the search of mass data storage devices;⁵⁹ the remote search of computer equipment;⁶⁰ and data preservation orders.⁶¹ In order to execute these measures, third parties are obliged to cooperate with the Public Prosecution Service or with the police, if served with a judicial warrant or in emergency situations. The same legal regime applies to ‘any person who knows how the computer system works, or the measures applied to protect the computer data contained in it’. Therefore, individuals are also required to cooperate under the obligation to keep the secrecy of the activities requested, being liable for contempt of court if they refuse to do so.⁶² For that reason, even though companies voluntarily cooperate, most of them usually ask for a judicial order

⁵⁷ Art. 588 ter j (1) CCP Electronic data held by service providers or persons facilitating communication in compliance with the legislation on retention of data relating to electronic communications, or on their own initiative for commercial reasons, or other type, and which are linked to communications processes.

⁵⁸ Art. 588 quinques (b) (3) CCP provides that the providers, agents and persons referred to in Art. 588 ter (e) are under the obligation to give the assistance and the cooperation needed to the judge, the Public Prosecution Service and members of the judiciary police appointed to carry out the investigative measure, to facilitate compliance with the orders ruling tracking, with a warning about committing the offence of contempt of court if they do not do that.

⁵⁹ Art. 588 sexies (c) (5) CCP states that the authorities and agents in charge of the investigation may order any person who knows about how the computer system works, or the measures used to protect the computer data contained on it, to provide such information as is necessary, if this does not cause a disproportionate burden on the affected party, with a warning about committing the offence of contempt. This provision will not apply to the investigated person or accused or to any other individual who is exempt from the obligation to testify due to being a close family member of the accused, and, in accordance with Art. 416.2, other individuals that are not under the duty of testifying due to their professional secrecy.

⁶⁰ Art. 588 septies (b) (1) CCP states that the service providers and persons indicated in Art. 588 ter (e) and the owners or those responsible for the computer system or database subject to search will be under the obligation to provide the investigating agents with such cooperation as is necessary to carry out the measure and access the system. Furthermore, they are under the obligation to provide assistance as needed so that the data and information gathered may be examined and visualised.

⁶¹ Art. 588 octies CCP establishes that the Public Prosecution Service, or the judiciary police, may require any individual or incorporated entity to preserve and protect specific data or information included on a computer system which they have had access to until the relevant judicial authorisation is obtained.

⁶² Art. 588 ter (e) (2) CCP.

before submitting the information requested, even when the information requested does not require a prior judicial decision by law.⁶³

The duty to cooperate applies, then, to real-time or stored data and, in general, to all types of such data (content, traffic, location, etc.). However, no warrant is required when the data is *user data* such as billing information. On the other hand, the law allows the police to hire private individuals or companies to decrypt the information hosted in a smartphone or to break the password to get access to the necessary information when this access is not achievable for public authorities.⁶⁴

Data requested by judicial order for telecommunications interception should be sent to the central computer of the Civil Guard or the National Police Headquarters in Madrid. The regulation on the conditions for the provision of electronic communications services compels the providers to prepare several interfaces through which the intercepted electronic communications and the information related to the interception can be transmitted to the reception centres (LEAs' headquarters).⁶⁵ The characteristics of these interfaces and the format for their transmission to these centres are set by the Ministry of Industry, Tourism and Trade through Ministerial Orders that comply with European Telecommunications Standards Institute (ETSI) technical specifications (e.g., ETSI standards for Lawful Interception and Requirements of Law Enforcement Agencies).

15.4.1 *Data Location and Territorial Criteria*

In accordance with Article 588 sexies (c) of the CCP 2015, the judicial warrant should define the scope and the grounds of the specific measure for which the order is addressed. However, paragraph 3 warns that, when the required data is stored in another computer system or device that forms a part of it, the warrant could be extended to the non-specified device that is being searched, provided that the required data is lawfully accessible through the initial electronic system, and it is easily available. However, this extension of the searched area not initially authorised must be made known to the judge. In cases of urgency, both the police and the prosecutor should report the action taken to the judge immediately, and at least within the next twenty-four hours the judge should be informed of both the search as it was carried out and its result. The competent judge could then revoke or confirm such investigative measures within a maximum of seventy-two hours from when the interception was ordered.

⁶³ It is usually a 'policy' of those companies. Article 118 of the Spanish Constitution sets a general rule of collaboration with the justice system, but Article 18.3 of the Constitution demands a judicial order when the action can be considered an interference in the secrecy of communications.

Although data requested by the police is not considered to be personal data under Article 18.3 of the Constitution and therefore does not require a judicial warrant, most companies ask the police for such a warrant anyway.

⁶⁴ See also Section 15.5. Art. 588 ter (e) (1) CCP states that

[a]ll the providers of telecommunications services, of access to a telecommunications network or of information society services, and any person who, in any way, contributes to facilitating communications via the telephone or by any other online, logic or virtual communication media or system, are obliged to provide the judge, the Public Prosecutor and the officers of the Judicial Police appointed to carry out the measure, with the assistance and collaboration required to facilitate the execution of telecommunications intervention orders.

⁶⁵ Real Decreto 424/2005 por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios (Regulation No. 424/2005 on the conditions for the provision of electronic communications services, universal service and users protection), Royal Decree 15 April 2005, BOE 29 April 2005, www.boe.es/buscar/act.php?id=BOE-A-2005-6970.

The power to extend a search order to other computer systems when the system is in a foreign jurisdiction, as ruled in the Budapest Convention Articles 19(2) and 32, is a very important step towards the investigation of cybercrimes; however, it comes with certain limitations. Article 19(2) allows the search of a computer to be extended to other computer systems, but only if those other systems are in *its territory*.⁶⁶ Article 32 of the Convention authorises trans-border access to the data stored, but only in the case that the stored data is publicly available or if the party obtains *the lawful and voluntary consent of the person who has the lawful authority to disclose the data* to the party through that computer system. The Explanatory Report of the Convention (paragraphs 293 and 294) openly acknowledges that ‘the drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. On one hand, this was due to a lack of concrete experience with such situations to date; and, on another hand, this was due to understanding that the solution often connects to the precise circumstances of the individual case, thereby making it difficult to formulate general rules.’ For that reason, and in the absence of a detailed explanation of what is meant by an *authorised person*, questions remain about the admissibility or otherwise of trans-border records ordered by a judicial authority when it comes to accessing information stored on computers that are not an *open source*.⁶⁷

In comparison with other state parties, there is no statutory provision in Spain similar to Article 125(j) of the Dutch Criminal Procedure Code⁶⁸ or Article 25 of the Portuguese Law on Cybercrime;⁶⁹ therefore, it is not expressly provided that foreign authorities must be informed of that access by Spanish LEAs, especially if the information could be found in open sources or with the consent of the affected subject. In that sense, it could be considered that the *legal consent* referred to in Article 32 of the Budapest Convention would be equivalent to judicial authorisation

⁶⁶ See Council of Europe, Explanatory Report to the Convention on Cybercrime, ETS No 185, 23 November 2001, para. 195, <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

⁶⁷ See M. Gercke, *Understanding Cybercrime: A Guide for Developing Countries* (Geneva: International Telecommunication Union (ITU), 2009), 207, www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cyber-crime-guide.pdf. See also the Explanatory Report, para. 293: ‘they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data’. In favour of cross-border searches, see J. L. Goldsmith, ‘The Internet and the Legitimacy of Remote Cross-Border Searches’ (2001) *University of Chicago Legal Forum*, Public Law and Legal Theory Working Paper No. 16, <http://papers.ssrn.com/abstract=285732>.

⁶⁸ Dutch Code of Criminal Procedure, s. 125j:

In the case of a search, a computerised device or system located elsewhere may be searched for data stored in that device or system that is reasonably required in order to reveal the truth from the place where the search takes place. If such data is found, then it may be recorded. The search shall be limited to the extent that the persons, who normally work or reside at the place where the search is being conducted, have access thereto from that place with the consent of the person entitled to use the computerised device or system. (Translation extracted from the website of the European Judicial Training Network (EJTN), www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenien/WetboekvanStrafvordering_ENG_PV.pdf)

⁶⁹ Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa (Cybercrime Law transposing for the internal legal order the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, and adapting the internal law to the Convention of the Council of Europe on Cybercrime), 15 September 2009, No. 109, www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis. Article 25 states:

The competent foreign authorities without prior request from the Portuguese authorities, in accordance with the rules on transfer of personal data provided by Law No. 59/2019 of 8 August, may: (a) access data stored in a computer system located in Portugal, where publicly available; (b) receive or access through a computer system located in its territory, the data stored in Portugal, through legal and voluntary consent of the person legally authorised to disclose them. (Personal translation)

See also Duarte Rodrigues Nunes, ‘The Means of Obtaining Evidence Provided by the Portuguese Cybercrime Law (Law No. 109/2009 of 15 September 2009)’ (2018) 24 *Comparative Law Review* 249–286.

issued by a Spanish judge, and that the voluntary consent of the authorised person would be tantamount to a tacit consent when the computer equipment under examination is configured in such a way that the judicial authority in charge of examining the equipment can access those virtual hard drives hosted abroad, the email inbox and so on. In any case, if the provider is based in Spain and the owner of the data is also in Spain, it would not matter where the data is located.

At present, there is no case law regarding cross-border searches and seizures by Spanish authorities based on Article 32 of the Cybercrime Convention. However, the courts have declared that such actions would be subject to the safeguards and guarantees of the Spanish law. For instance, the National Court (*Audiencia Nacional*)⁷⁰ ruled on 30 April 2009 that a judicial control was needed if a criminal investigation was launched in order to obtain a piece of evidence abroad. According to this judgment, the enforcement of such investigative measures by foreign authorities does not exempt the Spanish judge from complying with the basic guarantees established in the Spanish legal system.⁷¹

Similarly, some scholars have also proposed application of the regime of interception of telecommunications without the technical assistance of another member state settled in Article 20 and following of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000.⁷² However, that legal possibility can be used only under the following conditions:

- (a) informing the member state prior to the interception in cases where the requesting member state knows that the suspect is on the territory of the notified state – however, the interception cannot be executed until the measure has been agreed to by another member state;
- (b) if the interception is already taking place, informing the member state immediately after the requesting member state becomes aware that the subject is present on the territory of the notified member state.

That said, this conventional regulation is designed solely for the cross-border interception of communications and not for any other investigative measure with extraterritorial effects (i.e., recording of the memory of electronic devices, seizure of content data stored on servers used as virtual hard drives, connection strings, connection data preserved by some websites, etc.).

15.4.2 Cross-Border Cooperation between LEAs and Service Providers

Unlike the principle of extraterritorial criminal jurisdiction, which enables Spanish jurisdiction to prosecute certain crimes committed abroad,⁷³ the investigative measures carried out by LEAs

⁷⁰ The *Audiencia Nacional* is not the Supreme Court, although its jurisdiction covers all Spanish territory. It is a Court with three chambers (criminal, administrative and labour). The criminal chamber competences are regulated by Art. 65 of the Ley Orgánica 6/1985 del Poder Judicial ((Organic) Law No. 6/1985 on the Judiciary, LOPJ), 1 July 1985, BOE 2 July 1986) and its judgments are referred to as ‘SAN’. SAN 2051/2009, 30 April 2009, FJ 3.A. Cuestiones Previas (iii) (b): ‘The fact, given the globalization of communications, that the search of electronic communications located in any other country is technically possible does not mean that the legal general regime which they are related to for their constitutional validity in Spain does not apply. Therefore, we do not necessarily consider that it is feasible to replace the judicial control of the Spanish judge, in relation to a measure that affects any citizen under its jurisdiction, with another foreign judge order, according to its own law which in any case should be taken into account, that may act only as complementary to the Spanish Law.’ (Note to the reader: *cuestiones previas* are procedural exceptions or waivers invoked by the defence that the Court must analyse before looking at the merits of the case.)

⁷¹ Ortiz Pradillo, ‘Problemas procesales’, 213.

⁷² J. Pérez Gil, ‘Convenio de Asistencia Judicial penal’, in M. Jimeno Bulnes (ed.), *La cooperación judicial civil y penal en el ámbito de la Unión Europea: instrumentos procesales* (Barcelona: Bosch, 2008), 291. See also Ortiz Pradillo, ‘Problemas procesales’, 214.

⁷³ Provided for in Art. 22 LOPJ.

and judicial authorities are purely territorial, with some exceptions established by the rules of international judicial cooperation (e.g., undercover agents acting abroad, joint investigation teams, or interception of telecommunications without the necessary technical assistance of the country where the communication occurs). Telecommunications interception can be ordered when at least one of the people involved in the communication is within the Spanish territory, or when both individuals are abroad, but the operator that supports the communication is subject to Spanish law.

This was well illustrated in an interesting case of interception of communication decided by the Supreme Court in a judgment of 14 September 2016. In this case, the individuals involved were in Tangier (Morocco), but the software used in Spain for the interception of communications (SITELE) managed to capture concrete pieces of conversations. The court considered that the interception should be legally valid, without the necessary permission from the Moroccan authorities, because the telephone handset was property of Spanish citizens, and by chance it was still operated by a Spanish service provider whilst abroad. In addition, the interception was ordered by a valid judicial warrant even when the interception crossed territorial borders from where the communication was sent and received.⁷⁴

However, beyond the scope of situations illustrated by this case, the Spanish law requires the use of instruments of international judicial cooperation – mutual legal assistance (MLA) agreements or mutual recognition EU instruments – in order to request the cooperation of foreign service providers. Law No. 23/2014 on mutual recognition of criminal decisions in the European Union offers the legal framework for requests formulated by the Spanish authorities and in relation to their reaction to requests received from other member states.

Furthermore, no legal rule impedes LEAs from directly contacting service providers located in other countries in order to obtain information. Although there is no jurisprudence in that respect, Spanish authorities usually contact service providers abroad directly, but also indirectly through legal representatives, branches or subsidiaries located in Spain.

Some compelling ways of requesting service providers, even when their data centres are located abroad, can be found in Law No. 34/2002 on Information Society Services and Electronic Commerce.⁷⁵ In that law, Article 2.1(II) provides that their provisions are enforceable against those service providers who have a registered office in Spain. Furthermore, Articles 2.2 and 4 extend the definition of service provider to cover not only those that have a permanent establishment located in Spain but also service providers that *direct their services specifically to Spanish territory*.

Finally, if this interpretation is followed, service providers located abroad (foreign service providers) should comply with the cooperation duties of Articles 588 ter, sexies and septies CCP 2015. However, there is no judicial decision that could allow us to conclude that a foreign service provider must necessarily cooperate with the Spanish authorities, under warning of being subject to the sanctions provided for in Law No. 34/2002. In that sense, the key would lie in knowing how to link a judicial attribution criterion to the concept of *service provider* in a specific jurisdiction, even if the data is not hosted there or there is no branch or premises in that jurisdiction.

⁷⁴ STS 704/2016, 14 September 2016, FJ 2.5.

⁷⁵ Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico (Law No. 34/2002 on Information Society Services and Electronic Commerce), 11 July 2002, BOE 12 July 2002, www.boe.es/buscar/act.php?id=BOE-A-2002-13758.

15.4.3 *Enforcement of the Transfer Order and the Consequences of Refusal to Cooperate*

Requests must be complied with according to the deadlines provided by the judge or within seven calendar days counted from 8 a.m. on the calendar day following the one in which the obliged entity received it (Article 7 Law No. 25/2007). Failure to comply with the obligations provided for in Law No. 25/2007 will be sanctioned in accordance with its provisions and the regime of sanctions laid down in General Telecommunications Law No. 32/2003, which provides for financial penalties ranging from 50,000 to 20,000,000 euros or disqualification of up to five years of service providers, which results in preventing them from offering services in relation to any networks or the provision of electronic communication services during that time.

While the risk of those penalties seems to be sufficiently compelling, service providers tend to reject requests from the police that are not issued by a judge, as this is mandated already by the Spanish Constitution (Article 18) and by the relevant law (Law No. 25/2007). The Supreme Court case law and the guidelines of the National Prosecution Office further confirm the necessity of a judicial warrant.

15.5 SECURITY MEASURES AND DECRYPTED DATA

Regarding the enforcement of any judicial warrant by LEAs, there is a legal general duty for all citizens, either individuals or legal entities, to cooperate with the Spanish justice system as required by Article 118 of the Constitution as well as by Article 17.1 of (Organic) Law No. 6/1985 on the Judiciary (LOPJ). This rule plays an important role in establishing the scope of cooperation duties for service providers and, especially, for third persons, in relation to the specific investigation measures that LEAs could carry out, as established in the above-cited sections of Article 588 CCP 2015.⁷⁶ Thus, when LEAs are enforcing a judicial warrant ordering an interception of electronic communications, there is a general duty for anyone, service providers or third persons, to provide them with assistance and the necessary cooperation. More specifically, Article 39 of the General Telecommunications Act No. 9/2014 expressly states that the legally bound parties must always have one or more interfaces ready through which electronic communications may be intercepted and transmitted to the authorities. The characteristics of these interfaces and the format for transmitting the communications intercepted are subject to the technical specifications established by the Ministry of Industry, Energy and Tourism. If the obliged entities applied any compression, encryption or other kind of encoding to the intercepted communications, they must hand over the communications unprotected. The intercepted communication must be sent to the interception reception centre with the same quality that the recipient of the communication had obtained originally.

Regarding access to the information required and the forensic analysis of computer devices, Article 588 sexies (c) CCP 2015 expressly provides that the authorities in charge of the investigation are empowered to order any person with knowledge of computer systems or knowledge regarding the encryption codes used to conceal the data contained to provide the necessary information, as long as this does not cause a disproportionate burden on the affected person. The latter mentioned safeguard for manufacturers, which could present an exception to the legal duty to provide the necessary information to LEAs (when it causes a disproportionated burden on them), appears as an important issue when it is compared to other jurisdictions' practices, for

⁷⁶ As explained in Section 15.4.

instance in comparison with the practice exemplified by the well-known US case in relation to Apple (San Bernardino case).⁷⁷ In this case, the Federal Bureau of Investigation (FBI) requested the assistance of Apple for unlocking the smartphone of a suspected terrorist through a judicial warrant, which the manufacturer refused by stating that it would impose a substantial burden on it. Ultimately, the US Department of Justice dropped the motions after the FBI found another company to provide the software needed. Had that case occurred in Spain,⁷⁸ it would have reached the same result but through a different process. One of the main characteristics of the new measures related to cybercrime investigation is their extensive nature, since they basically concern activities related to social communication. However, when Article 588 septies (b) refers to owners or persons responsible for the computer system or database object of the investigation measure, it refers not to the manufacturers (e.g., Apple in the above-mentioned San Bernardino case) but to those who manage a computer system or database, meaning that the duty of cooperation would be linked to the condition of having knowledge of the operation of the system.

On the other hand, still comparing with the example of the *FBI v. Apple* case, if the only way for the Spanish regulations – aimed at providing the necessary information to obtain the required data – would have been the creation of an ad hoc digital solution (available only to the manufacturer), the law would have not provided for an express duty of cooperation for service providers or any other third person.

To zoom in on this example: Apple in Spain has a double condition, as a manufacturer and as a service provider of the information society (iTunes service). Accordingly, the company would have been subjected to Spanish law, and then would have had the duty to facilitate the access in clear language to instant messaging or through any other form of information or communication preserved thanks to the interaction of iTunes, which would lead to the indirect result of opening the doors to the rest of the information.⁷⁹ Nevertheless, as explained already, the Spanish law has established a specific exception from the obligation of cooperation when there is a disproportionate burden on the person or manufacturer affected by the measure (which was actually the defence used by Apple in the San Bernardino case).⁸⁰

In several cases, the Spanish LEAs requested the cooperation of companies specialised in hacking of devices. For instance, the company Cellebrite, which is a manufacturer of one of the most powerful uploading data tools for mobile phones known as UFED, offered a service

⁷⁷ In 2016, a judge of the District Court for the Central District of California ordered Apple to create a software enabling the FBI to bypass the security encryption code of an iPhone belonging to Mr Farook, suspected of a terrorist attack in the so-called San Bernardino shooting. The FBI did not clearly state which data was sought, expecting to find information related to the terrorist crime committed by Mr Farook or any detail about a possible terrorist network. Apple refused to comply with the FBI's request, despite the FBI having obtained a warrant and thus having a legal right to search the phone. The company objected to the court forcing it to reverse engineer its encryption because doing so would impose a substantial burden on the company and force it to create a new technical solution that would violate its products and its consumer promise of privacy, seriously threatening its position in the market. For further information about the case, see Ann Kristin Glenster, 'Decrypting Apple: Making Technology Companies the Referees of Law Enforcement on Privacy', *JOLT Digest*, 6 June 2017, <https://jolt.law.harvard.edu/digest/decrypting-apple-making-technology-companies-the-referees-of-law-enforcement-on-privacy>.

⁷⁸ The law gives LEAs and judges the power to request any person who knows the computer system to provide the information necessary for the execution of the measure.

⁷⁹ J. L. Rodríguez Lainz, '¿Podría un juez español obligar a Apple a facilitar una puerta trasera para poder analizar información almacenada en un iPhone 6?' (2016) 8729 *Diario La Ley* 8.

⁸⁰ That legal strategy used by Apple was based on the risk of damage to its commercial reputation, the absence of a rule that specifically empowers the judicial authority to impose that duty of cooperation and the risk of affecting the security of all its systems as a result of the creation of what was defined as an authentic back door. In relation to giving the FBI access to customers' data through password-protected iPhones, the FBI officials called it the 'going dark' problem when arguing that all data should be accessible with a warrant. Apple insisted that the problem was called

called CAIS dedicated exclusively to decrypting the contents of the internal memory of mobile phones that store encrypted information (such as BlackBerry, iPhone and Samsung). This company was requested by the Spanish authorities to open such seized phones on several occasions.⁸¹

Third parties must provide the necessary information to assist in removing obstacles or difficulties with which a specific computer system is equipped, either by its own logical configuration or design, or by the activation of its mechanisms or any other system of protection that impedes access to the data contained. The same applies when the computer or electronic device is found at the suspect's home during the enforcement of a search and seizure warrant. In this case, the police may request the suspect or any other person living in the searched home to provide the password of the electronic device; if they do not provide that information, LEAs are empowered to order a third party (who could be a hacker or expert) to break the password and facilitate access to the information kept in the computer or electronic device.

In sum, what characterises and defines the powers of LEAs given by Article 588 sexies CCP is the possibility to legally order anyone for 'a facilitation of knowledge', not a 'facilitation of means or tools'. Therefore, the information requested could be either in the form of disclosure of access codes, if they are known, or in the form of technical advice providing accurate information, so that any obstacle that impedes access to the memory of the device can be removed.⁸²

In relation to remote searches, Article 588 septies CCP 2015 provides for a duty of cooperation that goes beyond what has been explained just now as 'facilitation of knowledge'. In section septies of Article 588, service providers and any of the persons indicated in Article 588 ter (e),⁸³ the owners or anyone responsible for the computer system or database under investigation, are obliged to aid and cooperate with LEAs, in order to facilitate *the necessary assistance aimed to enable the visualisation and examination of the gathered data*.

Furthermore, LEAs can use any technical means to identify any electronic devices which are the subject of judicial investigation. In that sense, Article 588 ter (l) enables LEAs to use technical devices that allow access to data or identification codes or technical labels of a telecommunication device or any of its components, such as the IMSI or IMEI numbering, and to the use of any technical means that, according to the state of technology, are valid to identify the communication equipment used to gain access to the telecommunications network.

So far there has been no publicly known case in which a company was requested to change its security protocols in order to enable LEAs to intercept communications. In fact, due to the ETSI standards, if the computer system is operating in Spain, the communication is intercepted by the operator and sent through secure channels and in a readable language to the operating centres of the Civil Guard and the National Police.

a 'back door' and that it would hurt security for everyone who uses the device. In that sense, a back door is a means to access a computer system or encrypted data that bypasses the system's customary security mechanisms.

⁸¹ See P.O.D. 'Desbloqueado el móvil de Diana Quer', *El País*, 6 July 2017, https://elpais.com/politica/2017/07/06/actualidad/1499325032_475830.html and S. Fernández, '¿Por qué ha tardado casi un año la Guardia Civil en conseguir desbloquear el móvil de Diana Quer?', *Xataka móvil*, 6 July 2017, www.xatakamovil.com/apple/por-que-ha-tardado-casi-un-ano-la-guardia-civil-en-conseguir-desbloquear-el-movil-de-diana-quer.

⁸² Rodríguez Lainz, '¿Podría un juez español?', 6.

⁸³ All providers of telecommunications services, of access to a telecommunications network or information society services, and any person who, in any way, contributes to facilitating communications via the telephone or by any other online, logic or virtual communication media or system, are under the obligation to provide the judge, the Public Prosecution Service and members of the judiciary police appointed to carry out the measure, with the assistance and cooperation necessary to facilitate the interception.

15.6 ADMISSIBILITY OF ELECTRONIC EVIDENCE

In broad terms, all the electronic evidence obtained by virtue of any technological investigation measures can be used as incriminating evidence in a criminal proceeding. As such, any procedural party can challenge its admissibility and request its exclusion if that specific piece of evidence has been obtained unlawfully.⁸⁴

In relation to the standards of proof, all digital evidence presented before the courts must meet the standards of credibility and authenticity. On some occasions (e.g., if the information results from a judicial interception) there are international standards for the presentation of this information (ETSI standards). Furthermore, for instance in cases of forensic device analysis, the experts who prepared the reports may be subject to cross-examination, and the defence usually requests information in relation to the computer software used for the decryption dump.

15.7 CONCLUSIONS

This chapter was finalised when the e-Evidence Regulation had just been adopted.⁸⁵ One of the crucial elements of that Regulation is the establishment of a sort of simplified mutual recognition, which (more or less) excludes from the equation the receiving state (in the first place at least). The newly adopted Regulation will, for sure, raise interesting new questions. The point from which the debate must begin, however, seems to be not complicated but extremely simple: if a Spanish judge is bound by EU law and must recognise and enforce an Italian judicial decision as if it were his or her own resolution, would a Spanish service provider be equally bound by the European law? This would mean that, by virtue of the principle of mutual trust, a private entity located in Spain should trust the legitimacy of an order from an Italian judicial or police authority, and enforce it as such, that is, as if it were an order from a Spanish judicial or police authority.

The key to success of the new direct cross-border cooperation system is establishing that a private agency can follow up any request made by a foreign judicial or police authority, and that a judicial order should be considered equally admissible and binding (mandatory) in any jurisdiction as if it had been issued by the judicial or police authority of the country where the agency operates or has its headquarters. That is what the e-Evidence Regulation provides for, but the practice might be more complicated.

Finally, questions may arise regarding the admissibility of the collected evidence before the Spanish courts, considering that the Spanish law requires a judicial warrant in order to give evidentiary value to the data obtained. In the case of a cross-border investigation, if a piece of evidence requested by a Spanish judge has been gathered in a different country where a judicial warrant is not necessary, however legally obtained in the country from which the evidence was gained, in Spain the admissibility of that piece of evidence obtained by LEAs without judicial warrant may be problematic and unlawful.⁸⁶ Under the e-Evidence Regulation, which is based

⁸⁴ According to Art. 11.1 LOPJ, unlawful evidence is considered when any piece of evidence has been obtained with the intention of establishing a defendant's guilt by violating their fundamental rights or freedoms. In this case, any digital data obtained without the necessary judicial warrant could be considered unlawful; therefore, it should be excluded from the criminal process. However, as explained earlier, when circumstances of urgency and necessity arise, the judicial warrant could be issued afterwards and still be valid in relation to the lawfulness of the evidence obtained.

⁸⁵ Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191/118 (e-Evidence Regulation).

⁸⁶ C. Cuadrado Salinas, 'La efectividad de las pruebas penales obtenidas en el marco de la futura normativa europea relativa a la obtención y conservación de pruebas electrónicas' (2021) 5 *Revista General de Derecho Procesal* 20.

on direct cooperation, this problem should, however, be limited or nonexistent as EU law now determines when a court order is required – that is, for the production of traffic or content data – and this requirement should be met by the issuing authority.⁸⁷ The latter sends the European production order directly to the foreign service provider, in principle without the intervention of the authorities of the member state of the service provider. The future will tell if the new system will nevertheless generate problems of admissibility of evidence and what other problems it will create when applied by Spanish LEAs.

⁸⁷ E-Evidence Regulation, Art. 4(2).

A Comparative Analysis of National Law and Practices

Unravelling Differences in View of EU-Wide Solutions

Stanisław Tosza and Vanessa Franssen

16.1 INTRODUCTION

In the wake of the adoption of the e-Evidence Regulation,¹ despite different instruments having a harmonising effect on national legislation, such as the Council of Europe Cybercrime Convention,² and years of cooperation in criminal matters, national systems in the European Union (EU) still diverge significantly when it comes to gathering digital or electronic evidence³ from providers of online or ‘network-based’⁴ services (in short: service providers). These differences will inevitably play a role in the process of putting the e-Evidence Regulation into practice and complementing its enforcement mechanism as far as this is left to the member states.⁵ They will also impact the negotiations on an agreement with the United States (US) under the CLOUD Act,⁶ and the implementation of the Second Additional Protocol to the Cybercrime Convention.⁷ Conversely, these processes will also have an impact on national legislation.

The objective of this chapter is to examine national legislations in the EU member states selected for this research – Belgium, Estonia, Germany, Ireland, Luxembourg, Poland and Spain – and reveal common patterns and differences in legal rules and their practical application when gathering electronic evidence for criminal investigations. The chapters presenting EU national legal systems in this book were prepared according to a uniform structure, which this comparative chapter will replicate.

To set the scene, it will first examine two aspects that are of paramount importance for understanding the rules on gathering electronic evidence: on the one hand, the terminology applied to such evidence as well as the categorisation of data and service providers (Section 16.2), and on the other, the rules on data retention (Section 16.3). The latter aspect naturally affects the ability of law enforcement to subsequently get access to the data that is being sought.

¹ Regulation (EU) 2023/154 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191/118 (e-Evidence Regulation).

² Council of Europe Cybercrime Convention, ETS No. 185, 23 November 2001.

³ As indicated in the Introduction, both terms are used interchangeably in this volume.

⁴ Term used by the EU legislator in the recently adopted e-Evidence Regulation, Recital 7.

⁵ See in detail Chapter 7, this volume.

⁶ Clarifying Lawful Overseas Use of Data Act of 2018, www.justice.gov/criminal-oia/cloud-act-resources. For more details, see Chapter 21, this volume; see also Chapter 7, this volume.

⁷ Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, CETS No. 224, www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty-num=224. At the moment of writing, already nineteen EU member states have signed the Protocol. For more details on the Protocol, see Chapter 8, this volume.

In a second step, we will examine the rules on gathering electronic evidence by law enforcement authorities (LEAs) themselves and from service providers in the selected member states in the national context and in a cross-border context, whether in cooperation with other countries or in an unmediated or direct way. In that context, we will analyse mandatory requests, but also voluntary cooperation of service providers (Section 16.4). The chapter will conclude with a reflection on the challenges for putting into effect the e-Evidence Regulation in view of the outcome of the comparative analysis.

16.2 TERMINOLOGY AND CATEGORISATIONS

Two elements are crucial for outlining the rules on gathering electronic evidence from service providers: how to define the object of the gathering – the data – and how to define the subjects of request for that data – the providers of different services. This section will examine different approaches of delineating both categories. We will first examine how data appears in the rules concerning gathering and admissibility of evidence (Section 16.2.1). In a second step, we will analyse how data is defined and categorised (Section 16.2.2), before exploring different approaches to defining the service providers which are under an obligation of cooperation to gather electronic evidence (Section 16.2.3).

16.2.1 *Data as Evidence*

Despite its undeniable importance these days for criminal investigations, relating not just to cybercrime offences but also to traditional crimes committed offline, the term ‘digital’ or ‘electronic evidence’ is defined nowhere in the law of the seven selected legal systems. At most, it can be inferred from a definition of the term ‘data’ in the parliamentary documents, as is the case in Belgium: digital evidence is ‘data that has been stored, processed and transmitted in an IT system’, and that is gathered for the purpose of evidence.⁸ Elsewhere, the term is described based on scholarly literature. For instance, in Polish legal doctrine, the term refers to data seized in an information system, stored on a data carrier or generated during an interception of communications.⁹

When it comes to *specific investigative measures for gathering digital evidence*, only a few legal systems seem to be well-equipped. Roughly speaking, the seven selected legal systems can be split up into three sub-groups. The first group encompasses legal systems where digital evidence is gathered mainly based on old rules on investigative measures which were designed for the pre-internet era.¹⁰ This is the case of Estonia,¹¹ Ireland¹² and Poland.¹³ This may seem surprising considering Estonia is regarded as an ‘advanced e-State’¹⁴ and the presence in Ireland of many European headquarters and data centres of major service providers, making it a ‘key jurisdiction for law enforcement access to the data held by those providers’.¹⁵ In Estonia, however, this approach is explained by the desire to make ‘rules of criminal procedure technology-neutral’¹⁶

⁸ Belgium, Chapter 9, 222.

⁹ Poland, Chapter 14, 374.

¹⁰ The only exception are the rules on access to retained data (see Section 16.3).

¹¹ Estonia, Chapter 10, 261–262.

¹² Ireland, Chapter 12, 309.

¹³ Poland, Chapter 14, 374.

¹⁴ Estonia, Chapter 10, 261.

¹⁵ Ireland, Chapter 12, 309.

¹⁶ Estonia, Chapter 10, 261.

and overall it is not considered problematic.¹⁷ Furthermore, in Ireland and Poland, the rules on gathering data are spread over different statutes and – for Ireland – common law rules,¹⁸ resulting in an incoherent legal framework.¹⁹

The second group applies a combination of old and modern rules. This holds true for Luxembourg where digital evidence is largely collected ‘on the basis of existing horizontal measures’ laid down in the Code of Criminal Procedure.²⁰ In addition, a few specific measures have been created, such as the quick preservation of data and the seizure of stored data (previously done on the basis of the provision relating to the seizure of devices).²¹

The third group, gathering Belgium, Germany²² and Spain, provides for a whole range of modern investigative measures that are tailored to the digital reality, thanks to (fairly) recent reforms of the Code of Criminal Procedure (2015 in Spain,²³ 2016 in Belgium²⁴ and several consecutive amendments in Germany). Belgian law provides for specific rules on the seizure of data, overt and covert searches and seizures in information systems, remote searches, online police infiltration and quick preservation of data, in addition to a whole range of cooperation duties for services providers.²⁵ In Spain, the Code contains a ‘comprehensive’ and ‘innovative’ set of investigative measures (such as interception of all types of electronic communications, Global Positioning System (GPS) tracking, the use of international mobile subscriber identity (IMSI) and international mobile equipment identity (IMEI) catchers, remote searches and digital undercover agents) to make criminal investigations more efficient.²⁶ Under German law, digital evidence can be collected, for instance, through search and seizure of data storage devices, production orders, remote searches and specific measures for telecommunications data.²⁷

Another interesting finding is that reforms of national criminal procedure were in several instances triggered by European and international obligations, in particular the Council of Europe Cybercrime Convention, the case law of the European Court of Human Rights (ECtHR) and EU law.²⁸ In a number of legal systems, the changes are (also) explained by the clear political will to meet the needs of law enforcement and/or the need to address developments in national case law.²⁹

With respect to the *admissibility of data as evidence*, most legal systems seem to struggle as digital evidence is not explicitly covered by the rules of evidence. This is especially the case in systems that have a closed catalogue of types of evidence. For instance, in Germany, the catalogue of potential evidence includes only statements by the accused, witness and expert statements, documentary evidence and inspections (enabling the ‘sensory perception of evidence’).³⁰ To fit into one of those categories, data or recordings must be transformed into evidence: for instance, a video may be shown and ‘perceived visually’; a text document stored in

¹⁷ Ibid., 264.

¹⁸ For example, Poland, Chapter 14, 375.

¹⁹ Ibid., 2–3; Ireland, Chapter 12, 310–311.

²⁰ Luxembourg, Chapter 13, 348.

²¹ Ibid., 348–349.

²² That said, German law also entails broad, generic cooperation duties, in addition to more specific cooperation duties for (different categories of) service providers. Germany, Chapter 11, 300–301.

²³ Spain, Chapter 15, 400–401.

²⁴ Belgium, Chapter 9, 221.

²⁵ Ibid., 221–222.

²⁶ Spain, Chapter 15, 400–401.

²⁷ Germany, Chapter 11, 290–295.

²⁸ For example, Luxembourg, Chapter 13, 348–349; Spain, Chapter 15, 401, 403.

²⁹ For example, Belgium, Chapter 9, 221; Spain, Chapter 15, 402–403.

³⁰ Michael Bohlander, *Principles of German Criminal Procedure*, 2nd ed. (Oxford: Hart, 2021), 146–163; Germany, Chapter 11, 289.

an information system can be printed and read as a document; other data may be examined by an expert who will be called as a witness.³¹

A similar situation can be found in Estonia, where a distinction is made between strict and free evidence. Strict evidence comprises any document and ‘other recordings’, which may cover stored data as well as real-time data collection to the extent that there is a report or recordings of the data.³² Stored data may also be considered ‘physical evidence’ when gathered on a data carrier.³³ It is, however, not possible to add an authentic copy of the data to the criminal file; only the inspection report of the analysis of the data can be included.³⁴ The Estonian courts further ruled that short message service (SMS), emails and ‘voice recordings of one’s own conversations’ fall into the category of strict evidence.³⁵ By extension, ‘any message in digital form can be used as evidence’.³⁶

In contrast, Belgium has ‘very open’ rules of evidence, hence the admissibility of digital evidence does not raise any particular problems.³⁷ All types of evidence are allowed.

Irish law, too, is quite permissive: while digital evidence is not recognised as a distinct category of evidence entailing separate safeguards, the rules of evidence do not exclude it either. In practice, though, the courts have set a high threshold for the use of digital evidence, requiring ‘appropriate authoritative evidence to describe the function and operation of the computer’.³⁸ This requirement is difficult to meet when data is delivered by foreign service providers. To date, this obstacle has been overcome only for data produced by US service providers, thanks to the mutual legal assistance (MLA) treaty between Ireland and the US, which certifies the function and operation of US providers’ information systems.³⁹

16.2.2 *Definition and Categories of Data*

In relation to digital evidence consisting of data, the research tried to get a better understanding of how data is defined and categorised in the seven EU member states. In addition, it questioned the categorisation of specific types of data that LEAs regularly seek to obtain in the context of a criminal investigation and that are likely to fit less easily into one of the ‘traditional’ data categories (e.g. login information, decryption keys and passwords, dynamic internet protocol (IP) addresses, draft and unread emails, communications in chat rooms and in the context of online games, as well as machine-to-machine data).

Most legal systems do not provide for a general *definition* of data, except for the term ‘personal data’ which is defined directly by the General Data Protection Regulation (GDPR).⁴⁰ Even when there is no explicit legal definition at national level, several national chapters hint at the influence of European law.⁴¹ Furthermore, in several systems, the term ‘data’ comes back in different legislations, which sometimes leads to practical problems. This is the case in Poland,

³¹ Germany, Chapter 11, 289.

³² Estonia, Chapter 10, 263.

³³ Ibid., 266.

³⁴ Ibid., 266.

³⁵ Ibid., 263.

³⁶ Ibid., 263.

³⁷ Belgium, Chapter 9, 222.

³⁸ Ireland, Chapter 12, 312.

³⁹ Ibid., 313.

⁴⁰ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1 (GDPR).

⁴¹ For example, Germany, Chapter 11, 296–297; Luxembourg, Chapter 13, 356; Poland, Chapter 14, 380–381.

where the term ‘computer data’ as defined by the Cybercrime Convention is used in the field of substantive criminal law, while the term ‘telecommunications data’ is applied in the context of criminal procedure and telecommunications law.⁴² In Irish law, reference to ‘data’ is made in data retention legislation and in legislation defining offences against information systems, each with their own scope of application.⁴³ In contrast, legislation regarding investigative measures such as search warrants and production orders contains more generic terms (e.g. ‘documents’, ‘records’ or ‘information’) which include computer data.⁴⁴

As far as *data categories* are concerned, the European Commission had already observed when preparing its e-evidence legislative package⁴⁵ that the definition of data categories ‘varies significantly among Member States’, even if the distinction between subscriber, traffic and content data comes back in several of them.⁴⁶ This is confirmed by our comparative research. Most legal systems indeed make a threefold distinction between data categories under the influence of the Council of Europe Cybercrime Convention or EU law (in particular the e-Privacy Directive⁴⁷ and the annulled Data Retention Directive⁴⁸), but these data categories sometimes coexist with other national terms (e.g. ‘telemedia usage data’ under German law;⁴⁹ or ‘telecommunications transmission’ under Polish law, which comprises the content of telephone conversations or other information sent over a ‘telecommunications network’⁵⁰). Moreover, a general or systematic categorisation of data seems to be missing in all legal systems.⁵¹ As a result, the same terms may cover different types of data, depending on the legal system.

The distinction between stored data and data in transmission also comes back in most legal systems, except for Belgium where the 2016 Internet Investigatory Powers Act erased this distinction as it was no longer considered fit for the digital era.⁵² Data in transmission (i.e. real-time or live communication) typically receives a higher level of protection (for instance, in Estonia⁵³ and in Spain⁵⁴). Due to this distinction, unread or draft emails cannot, for instance, be

⁴² Poland, Chapter 14, 380–381.

⁴³ Ireland, Chapter 12, 318.

⁴⁴ *Ibid.*, 318–319.

⁴⁵ European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, COM/2018/225 final – 2018/0108 (COD), 17 April 2018; European Commission, *Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings*, [2018] COM/2018/226 final – 2018/0107 (COD), 17 April 2018.

⁴⁶ European Commission, *Non-paper: Progress Report Following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace*, 15072/16, Brussels, 2 December 2016, p. 4.

⁴⁷ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), [2002] OJ L 201/37 (e-Privacy Directive).

⁴⁸ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, [2006] OJ L 105/54 (Data Retention Directive).

⁴⁹ Belgium, Chapter 9, 227; Germany, Chapter 11, 296–297. Please note also that the term ‘telemedia services’ would change to ‘digital services’ if the proposed law amending German law in light of the Digital Services Act is adopted (Germany, Chapter 11, 293).

⁵⁰ Poland, Chapter 14, 381.

⁵¹ For example, Ireland, Chapter 12, 319; Luxembourg, Chapter 13, 356.

⁵² V. Franssen and S. Tosza, ‘Vers plus de droits pour le justiciable sur internet? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l’information’, in V. Franssen and A. Masset (eds.), *Les droits du justiciable face à la justice pénale* (Limal: Anthemis, 2017), 223.

⁵³ Estonia, Chapter 10, 263–264.

⁵⁴ Spain, Chapter 15, 407.

intercepted, they can only be seized in Estonia,⁵⁵ Germany⁵⁶ and Spain.⁵⁷ Furthermore, the Spanish Supreme Court makes a distinction between static and dynamic data.⁵⁸

Nevertheless, upon a closer look at the content of the various data categories, some striking divergences come to the fore. For instance, in both Belgium and Germany, dynamic IP addresses can be obtained for the purpose of identifying the user based on the provisions regarding subscriber data, even if the data are formerly considered traffic data.⁵⁹ Interestingly, this approach corresponds to the one chosen by the EU legislator in the e-Evidence Regulation, which treats certain traffic data differently, namely ‘data requested for the sole purpose of identifying the user’ (for instance, IP addresses and the date and time of creation of an account).⁶⁰ In the Regulation, too, this data follows the regime of subscriber data.

Whereas login information such as usernames is regarded to be subscriber data,⁶¹ passwords and decryption keys are often not clearly categorized. In Belgium, they are ‘regarded as a means to facilitate searches of IT systems and interception rather than as a type of data’.⁶² Similarly, in Estonia, they are considered ‘access data’ that form ‘a separate undefined category’: although they provide access to content (e.g. email messages), the Supreme Court ruled that they are ‘as such . . . not revealing about the content of communications either and cannot be said to belong to the essence of content’.⁶³ By contrast, in Germany, passwords belong to the category of subscriber data.⁶⁴

Machine-to-machine data, which is becoming increasingly prevalent in a society where many objects are connected to the internet, is in some legal systems regarded as communications content data (e.g. Germany⁶⁵). However, in other systems, machine-to-machine data does not seem to belong to any of the three categories of communications data.⁶⁶

Finally, most legal systems seem to classify chat room communications and communications in the context of online games as content data.⁶⁷ Yet, the question whether this communication is ‘in transmission’ or already stored may impact the availability of traditional wiretapping measures.

To conclude, despite common labels, data can be categorised quite differently from one legal system to another, and even if certain types of data belong to the same category, the investigative measures to obtain them may vary considerably.

16.2.3 *Types of Service Providers*

Considering the central role of service providers in gathering digital evidence,⁶⁸ the comparative research aimed at delineating the personal scope of application of the cooperation duties

⁵⁵ Estonia, Chapter 10, 283.

⁵⁶ Germany, Chapter 11, 297.

⁵⁷ Spain, Chapter 15, 409.

⁵⁸ *Ibid.*, 409.

⁵⁹ Belgium, Chapter 9, 227; Germany, Chapter 11, 297.

⁶⁰ E-Evidence Regulation, Art. 3(10).

⁶¹ For example, Belgium, Chapter 9, 227; Germany, Chapter 11, 297.

⁶² Belgium, Chapter 9, 227.

⁶³ Estonia, Chapter 10, 264.

⁶⁴ Germany, Chapter 11, 297.

⁶⁵ *Ibid.*, 297.

⁶⁶ Belgium, Chapter 9, 227.

⁶⁷ For example, *ibid.*, 227; Germany, Chapter 11, 297; Poland, Chapter 14, 381; Spain, Chapter 15, 409.

⁶⁸ See also the Introduction, this volume.

imposed on service providers in the respective legal systems. To this end, the research sought to map the different terms that are used and identify their origin(s).

At first sight, the comparative analysis reveals a quite *diverse legal landscape*. Each legal system seems to use its own terms and definitions. For instance, in Germany, a distinction is made between providers of telecommunication services and ‘telemmedia service providers’.⁶⁹ In Estonia, the term ‘electronic communications undertakings’ is used in the Code of Criminal Procedure, by reference to the definition given in the Electronic Communications Act (ECA).⁷⁰ In the Luxembourg Code of Criminal Procedure, the old term ‘providers of telecommunication services’ can still be found.⁷¹ In Ireland, interception legislation refers to ‘authorised undertakings’, while data retention law applies to ‘service providers’. In both cases, the scope of legal duties is, however, limited to ‘traditional telecoms providers such as mobile phone or broadband providers’.⁷²

Nevertheless, upon a closer look, the definitions of national terms are *strongly influenced by EU legislation*. One could thus believe that EU law ensures some uniformity. Still, this uniformity is relative as it is limited to the scope of the respective EU law instruments, most of which do not relate (or relate only indirectly) to the field of criminal procedure. Some of these instruments refer to electronic communications services (and their providers) (the EU Electronic Communications Code⁷³ and the former Data Retention Directive), others to providers of information society services, distinguishing between several subtypes of services (the e-Commerce Directive⁷⁴ and the Digital Services Act),⁷⁵ or various other types of digital services (the NIS 1 and NIS 2 Directives).⁷⁶ This EU law patchwork is reflected at national level. For instance, the German term ‘telemmedia service providers’ largely corresponds to providers of information society services;⁷⁷ the Estonian term ‘electronic communications undertakings’ and the Polish term ‘telecommunications company’ echo the EU definition of providers of electronic communication services. Certain national experts rightly point to the fact that the distinction between the different types of service providers is not always clear-cut, creating grey zones;⁷⁸ others emphasize that LEAs have to check each time they ‘approach a given provider for particular data ... what legal act provides a basis for the provider’s operations; this will permit a proper legal definition of the provider, and will also make it possible to determine what obligations are imposed on the provider by that legal act’.⁷⁹

Moreover, despite their common origin, the application of EU-based terms also seems to diverge *in practice*. For instance, in Belgium, the scope of electronic communications service providers is broader in the Code of Criminal Procedure than in the legislation on electronic communications (which follows the EU definition) due to the principle of conceptual

⁶⁹ Germany, Chapter 11, 297–298.

⁷⁰ Estonia, Chapter 10, 271.

⁷¹ Luxembourg, Chapter 13, 357.

⁷² Ireland, Chapter 12, 319.

⁷³ Directive (EU) 2018/1972 of the European Parliament and the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), [2018] OJ L 321/36 (EU Electronic Communications Code).

⁷⁴ Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L 17/8/1, 17 July 2000.

⁷⁵ Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services and amending Directive 2000/31/EC of 19 October 2022 (Digital Services Act), [2022] OJ L 277/1.

⁷⁶ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, [2016] OJ L 194/1 (NIS Directive); Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L 333/80.

⁷⁷ Germany, Chapter 11, 297–298.

⁷⁸ Ibid., 298.

⁷⁹ Poland, Chapter 14, 383.

autonomy of criminal law.⁸⁰ De facto, all providers offering a service (e.g. food delivery) which is accompanied by an electronic communications service (e.g. an online app to order the food) are covered. Over-the-top (OTT) providers are thus also included.⁸¹ The Belgian experts therefore conclude that the notion of ‘providers of electronic communications services’ in Belgian criminal procedure rather corresponds to the broad definition of service providers in Article 1 of the Cybercrime Convention.⁸²

In Spain, a similar approach is taken. In the relevant section of the 2015 Code of Criminal Procedure, it is clearly stated ‘that the law applies to all providers and they all have a legal duty to cooperate with the authorities’.⁸³ In this context, the term ‘providers’ encompasses ‘not . . . only the internet service providers, but also . . . all providers of telecommunications services and information society services, as well as any other person who could contribute to facilitating communications’.⁸⁴ To the contrary, in Estonia, the EU definition of electronic communication services is applied in the context of criminal procedure, too.⁸⁵

In other legal systems, OTT providers are sometimes covered, depending on the type of cooperation duty. For instance, in Ireland, certain investigative measures (e.g. search warrants and production orders) apply more broadly, including information society service providers and OTT services.⁸⁶ In contrast, an interception order cannot be served upon a provider of information society services, even if the Irish Justice Department at some point expressed the desire to extend interception legislation to such providers.⁸⁷

Confronted with such national diversity, service providers operating in more than one EU member state inevitably face uncertainty about the extent of their cooperation duties under national law. In the criminal justice area, a ‘level-playing field’ for all service providers cooperating with law enforcement is still far away.

It remains to be seen if the new e-Evidence Regulation, which is so far the only EU instrument that directly concerns criminal procedure, will contribute to further approximation. Compared to pre-existing EU legislation, the Regulation has yet another scope of application, covering three types of service provider:⁸⁸ (1) providers of electronic communications services; (2) providers of internet domain name and IP numbering services; and (3) providers of other information society services that enable users to communicate with one another or that process or store data on behalf of their users, in which case the storage of data should be ‘a defining component of the service’ in point.⁸⁹ As argued elsewhere,⁹⁰ the application of the e-Evidence Regulation is likely to bring to the surface national disparities, in which case the Court of Justice of the European Union (CJEU) may be called upon to clarify the personal scope of the Regulation. Moreover, with respect to the third category of providers, practice will show whether the criterion that the storage is a ‘defining component’ of the service is easy to apply or, to the contrary, yields new uncertainties.

⁸⁰ Belgium, Chapter 9, 228.

⁸¹ *Ibid.*, 228–229.

⁸² *Ibid.*, 228.

⁸³ Spain, Chapter 15, 413.

⁸⁴ *Ibid.*

⁸⁵ Estonia, Chapter 10, 271.

⁸⁶ Ireland, Chapter 12, 327–329.

⁸⁷ *Ibid.*, 320.

⁸⁸ E-Evidence Regulation, Art. 3(3).

⁸⁹ *Ibid.*, Art. 3(3)(c)(ii).

⁹⁰ V. Franssen, ‘Cross-Border Gathering of Electronic Evidence in the EU: Toward More Direct Cooperation under the e-Evidence Regulation’, in V. Mitsilegas, M. Bergström and T. Quintel (eds.), *Research Handbook on EU Criminal Law*, 2nd ed. (Cheltenham: Edward Elgar, 2024), 193.

16.3 DATA RETENTION

Ever since the CJEU's ruling in *Digital Rights Ireland*,⁹¹ which invalidated the Data Retention Directive,⁹² the future of data retention and its compatibility with the Charter of Fundamental Rights of the EU (Charter) have been a hot topic of debate among policymakers, public and private stakeholders, as well as academics. In various subsequent judgments, the CJEU tried to further clarify the legal situation, putting forward detailed requirements for EU-proof data retention legislation, to the extent of almost adopting a legislative approach.⁹³ In essence, the CJEU ruled that general and indiscriminate retention of traffic and location data constitutes a 'very far-reaching' and 'particularly serious' interference in the rights to private life and the protection of personal data enshrined in Articles 7 and 8 of the Charter.⁹⁴ Such retention can be accepted only under very strict conditions to safeguard national security.⁹⁵ In other cases, the retention of traffic and location data must be limited to what is strictly necessary and targeted, based on objective and non-discriminatory criteria.⁹⁶ In addition, it can be justified only by the objective to fight 'serious crime',⁹⁷ a concept that is not (yet) defined at EU level.⁹⁸ The only exception is the IP address assigned to the source of an internet connection, which may be the only means of investigation to identify the suspect of an offence.⁹⁹ This type of data is considered less sensitive than other traffic data¹⁰⁰ and may be retained on a general and indiscriminate basis to combat serious crime 'for a period that is limited in time to what is strictly necessary'.¹⁰¹ In contrast, 'data relating to the civil identity of users of electronic communications systems' – a term that seems to correspond to the term 'subscriber data' – can be retained on a general and indiscriminate basis to fight any sort of crime.¹⁰² Furthermore, the CJEU also clarified the conditions for access to retained data by competent authorities¹⁰³ as well as the limits to the potential use of illegally retained data in national criminal proceedings.¹⁰⁴

In the view of many LEAs, this case law undermines the key role of data retention: making sure that digital traces are still available to law enforcement if a criminal investigation is opened at a later point in time against persons who were not suspects at the time of generating the data. Data retention is thus a 'proactive' measure without any connection to an ongoing criminal case, as opposed to, for instance, data preservation, which is a targeted investigative measure.¹⁰⁵

⁹¹ Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and others* [2014] ECLI:EU:C:2014:238 (*Digital Rights Ireland*).

⁹² Data Retention Directive.

⁹³ See, e.g., Joined Cases C-203/15 and C-698/15, *Telez Sverige AB* [2016] ECLI:EU:C:2016:970 (*Telez Sverige*); Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net* [2020] ECLI:EU:C:2020:791; Case C-623/17, *Privacy International* [2020] ECLI:EU:C:2020:790; Case C-746/18, *Prokuratuur* [2021] ECLI:EU:C:2021:152; Case C-140/20, *G.D. v. Commissioner of An Garda Síochána* [2022] ECLI:EU:C:2022:258; Joined Cases C-793/19 and C-794/19, *Spacenet AG and Telekom Deutschland GmbH* [2022] ECLI:EU:C:2022:702.

⁹⁴ See, e.g., *Telez Sverige*, para. 100; *La Quadrature du Net*, para. 177.

⁹⁵ *La Quadrature du Net*, para. 168.

⁹⁶ See, e.g. *Telez Sverige*, paras. 109–112; *La Quadrature du Net*, paras. 140–151.

⁹⁷ See, e.g. *Telez Sverige*, paras. 102 and 110; *La Quadrature du Net*, paras. 140–151.

⁹⁸ On this question, see, e.g., B. Flumian and V. Franssen, 'Le nouveau cadre légal en matière de conservation des données électroniques: "Old wine in new bottles" pour les autorités judiciaires?', in V. Franssen and A. Masset (eds.), *Le droit pénal et la procédure pénale en constante évolution* (Liège: Anthemis, 2022), 323.

⁹⁹ *La Quadrature du Net*, para. 154.

¹⁰⁰ *Ibid.*, para. 152.

¹⁰¹ *Ibid.*, para. 168.

¹⁰² *Ibid.*, para. 169.

¹⁰³ See, e.g., Case C-207/16, *Ministerio fiscal* [2018] ECLI:EU:C:2018:788; *Prokuratuur*, paras. 54–56.

¹⁰⁴ See, e.g., *La Quadrature du Net*, paras. 221–228; *Prokuratuur*, paras. 41–44.

¹⁰⁵ SIRIUS, *SIRIUS EU Digital Evidence Situation Report* (The Hague: European Union Agency for Law Enforcement Cooperation (Europol), 2022), 53–54.

The lack of an EU legal framework on data retention ‘leads to a loss of data’.¹⁰⁶ Without such data, it is more difficult and, in some cases, even impossible to investigate criminal offences.¹⁰⁷

A quite different reaction came from privacy experts and civil society.¹⁰⁸ They welcomed the CJEU case law as it sets important limits to large-scale surveillance and bulk data collection. Data protection authorities, too, have insisted that ‘any national data retention regime has to comply with the requirements of the Charter’¹⁰⁹ and argued that it ‘might be possible to provide a *limited yet effective* electronic communications data retention and access regime in a manner compatible with the Charter’.¹¹⁰

Confronted with this CJEU case law, policymakers at both EU and national level have been searching frenetically for a solution. At EU level, the European Commission and the member states have tried to find a common ground for new EU-wide data retention legislation,¹¹¹ but these attempts have not yet resulted in a legislative proposal. At national level, too, attempts to elaborate new solutions have been made. Our comparative research, however, demonstrates that those efforts are quite unevenly divided across the seven selected member states.¹¹²

Indeed, quite strikingly, a first group of member states continues to apply domestic data retention legislation as adopted to implement the Data Retention Directive, without making any substantial amendments, even if that legislation is clearly contrary to EU law as interpreted by the CJEU. This is the case for Estonia,¹¹³ Poland¹¹⁴ and Spain.¹¹⁵ In all three member states, the

¹⁰⁶ Ibid., 6 and 54.

¹⁰⁷ Ibid., 10 and 44–47.

¹⁰⁸ See, e.g., O. Lynskey, ‘Joined Cases C-293/12 and 594/12 Digital Rights Ireland and Seitlinger and Others: The Good, the Bad and the Ugly’, *European Law Blog*, 8 April 2014, <https://europeanlawblog.eu/2014/04/08/joined-cases-c-29312-and-59412-digital-rights-ireland-and-seitlinger-and-others-the-good-the-bad-and-the-ugly/>; J. Sajfert, ‘Bulk Data Interception/Retention Judgments of the CJEU – A Victory and a Defeat for Privacy’, *European Law Blog*, 26 October 2020, <https://europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/>; EDRi, ‘Civil Society Calls for a Proper Assessment of Data Retention’, 23 July 2019, <https://edri.org/our-work/civil-society-calls-for-proper-assessment-of-data-retention/>.

¹⁰⁹ European Data Protection Supervisor (EDPS), *Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*, 24 April 2017, p. 21, https://edps.europa.eu/data-protection/our-work/publications/opinions/eprivacy-regulation_en.

¹¹⁰ EDPS, Pleading notes, Joint hearing in Case C-623/17 (*Privacy International*) with Joined Cases C-511/18 and C-512/18 (*La Quadrature du Net and Others*) and Case C-520/18 (*Ordre des barreaux francophones et germanophone and Others*), 9–10 September 2019, p. 8, original emphasis, https://edps.europa.eu/data-protection/our-work/publications/court-cases/edps-pleading-hearing-court-justice-cases-c-62317_en.

¹¹¹ See, e.g., European Commission, Directorate-General for Migration and Home Affairs, C. Dupont, V. Cilli, E. Omersa et al., *Study on the Retention of Electronic Communications Non-content Data for Law Enforcement Purposes: Final Report* (Milieu Study) (Brussels, Publications Office, 2020), 94–97, <https://data.europa.eu/doi/10.2837/384802>; A. Juszczak and E. Sason, ‘Recalibrating Data Retention in the EU: The Jurisprudence of the Court of Justice of the EU on Data Retention – Is This the End or Is This the Beginning?’ (2021) *Eu crim*, s. IV.4, <https://doi.org/10.30709/eu crim-2021-020>. In spring 2023 a ‘High-Level Expert Group on access to data for effective law enforcement’ was created, chaired by the European Commission and the member state holding the presidency of the Council of the EU. The High-Level Expert Group is expected to propose, by mid-2024, ‘recommendations for the further development of Union policies and legislation to enhance and improve access to data for the purpose of effective law enforcement. In this context: contribute to integrating a law enforcement perspective, including privacy and data protection requirements, in all relevant EU policies and actions (“security by design”).’ It identified data retention, along with encryption and anonymisation, as the most pressing issues to address. High-Level Expert Group on access to data for effective law enforcement, *Scoping Paper*, annex to Presidency of the Council of the EU, ST-8281-2023-INIT, Brussels, 13 April 2023, pp. 3 and 5, <https://data.consilium.europa.eu/doc/document/ST-8281-2023-INIT/en/pdf>.

¹¹² This confirms earlier studies. See, e.g., EDRi, ‘Eurojust: No Progress to Comply with CJEU Data Retention Judgments’, 29 November 2017, and the references made there, <https://edri.org/our-work/eurojust-no-progress-to-comply-with-cjeu-data-retention-judgements/>; Milieu Study, 15.

¹¹³ Estonia, Chapter 10, 267 and 270–271.

¹¹⁴ Poland, Chapter 14, 376–377.

¹¹⁵ Spain, Chapter 15, 403.

reported data retention regime is still general and indiscriminate in nature, involving both subscriber and traffic data. For instance, in Estonia, the Supreme Court ‘unequivocally stated that Article 111(2) of the ECA, which requires the indiscriminate mass retention of traffic and location data by the providers of telephone or mobile telephone services and telephone network and mobile telephone network services, is in conflict with EU law’.¹¹⁶ Nevertheless, according to the Ministry of Justice, this ‘does not automatically mean that the provision would not be valid. Moreover, the Ministry noted that there is no clarity on the interpretation of the CJEU ruling at EU member state level and that there are member states where a general and uniform retention regime for communications data continues to be in place.’¹¹⁷ Since then some punctual amendments have been made to the ECA, which entered into force in January 2022, but they concern only the conditions for requesting and accessing retained traffic and location data.¹¹⁸ In Spain, courts have focused all their ‘attention in highlighting the high level of protection of the retained data and the specific requirements and safeguards included in order to obtain the access to the retained data’, but they ‘forget the original sin of our system: the disproportionate and indiscriminate retention regime contained in Law No. 25/2007’.¹¹⁹

In three other member states – Belgium, Luxembourg and Ireland – the legislator has tried to redesign domestic data retention legislation in a way to meet the concerns of the CJEU. In Belgium, this process resulted in the 2022 Data Retention Act, after two earlier Data Retention Acts, one of 2013 and another one of 2016, had been annulled by the Constitutional Court.¹²⁰ On the face of it, the new Act contains targeted data retention, based on geographical criteria. Upon a closer look, however, the new law ‘tries to stretch data retention to the maximum’ and de facto ‘large parts – if not the entire – Belgian territory is covered’.¹²¹

In Luxembourg, the legislative process at the time of writing the national chapter was still ongoing. However, the pending bill also proposes geographical criteria to limit the retention of traffic and location data to areas where the (likelihood of) commission of criminal offences is higher.¹²²

In Ireland, too, the legislator eventually faced the reality that existing data retention legislation, providing for indiscriminate data retention and access without independent authorisation, was not in conformity with EU law.¹²³ After *Digital Rights Ireland*, a first reform attempt was made in 2017, but the draft legislation failed to meet the CJEU standards and thus was received very critically.¹²⁴ The so-called *Dwyer* case¹²⁵ pushed the Irish government to rush new legislation through Parliament in 2022,¹²⁶ but the authors of the Irish chapter (Chapter 12) have serious doubts about its enforceability as the Irish government failed to notify the draft legislation to the European Commission as required by the Technical Regulations Information System

¹¹⁶ Estonia, Chapter 10, 270–271.

¹¹⁷ Ibid., 271.

¹¹⁸ Ibid.

¹¹⁹ Spain, Chapter 15, 403.

¹²⁰ Belgium, Chapter 9, 222–223. See also Flumian and Franssen, ‘Le nouveau cadre légal en matière de conservation des données électroniques’, 317–318.

¹²¹ Belgium, Chapter 9, 223–224. For a critical analysis of this new law, see, e.g., Flumian and Franssen, ‘Le nouveau cadre légal en matière de conservation des données électroniques’, 332–353; F. Dumortier and C. Forget, ‘La loi du 20 juillet 2022 ou l’art de dissimuler l’obligation de conservation systématique et indifférenciée des métadonnées’ (2023) 142 *Journal des tribunaux*, 405, 408–413.

¹²² Luxembourg, Chapter 13, 353–354.

¹²³ Ireland, Chapter 12, 313 and 316–317.

¹²⁴ Ibid., 313–314.

¹²⁵ In full: *G.D. v. Commissioner of An Garda Síochána*.

¹²⁶ Ireland, Chapter 12, 314.

procedure.¹²⁷ On the substance, the Communications (Retention of Data) (Amendment) Act 2022 would put an end to indiscriminate and general data retention and would introduce independent authorisation for access. On other points, the new law would, however, still not be fully in line with the case law of the CJEU.¹²⁸ At the same time, it is worth noting that the police still have the option to get access to data held by service providers by resorting to search warrants and production orders issued by the district court, which are pre-existing general measures.¹²⁹

Finally, Germany seems to be the only member state in our sample which currently has no data retention legislation in place. While the German legislator adopted in 2015 a data retention regime that is more limited in scope (with, for instance, very short retention periods) to meet the requirements of the German Federal Constitutional Court, this legislation was never enforced at national level¹³⁰ and the CJEU gave it the final dead blow in its *Spacenet* ruling in September 2022.¹³¹ In the absence of data retention legislation, German LEAs try to get access to traffic and location data by asking service providers to produce data they keep for commercial or technical purposes.¹³² This approach is compatible with Articles 5 and 6 of the e-Privacy Directive but makes LEAs highly dependent on the data that service providers decide to store. In practice, this creates only a short and uncertain window of opportunity for LEAs to access data.¹³³ Other solutions such as a 'login trap'¹³⁴ and resorting to more extensive police powers are also explored.¹³⁵

To sum up, the current data retention legal landscape is quite fragmented at national level, notwithstanding nearly ten years of CJEU case law on the matter. It is characterised by divergent legal rules and practices at national level. This obviously puts citizens' fundamental rights in danger, but also leads to continued legal uncertainty for the service providers addressed. The latter are still obliged to retain data in many member states even though those obligations are in violation of EU law, either manifestly (Estonia, Poland, Spain, as well as Luxembourg which continues to apply its 2010 legislation as long as the proposed bill has not been adopted¹³⁶) or potentially (Belgium and Ireland). For service providers operating in several member states (such as Orange or Telefónica), this complicates the exercise of their activities. The impact of this situation, however, goes way beyond the mere regime of data retention; it affects the way in which criminal investigations are conducted and digital evidence is gathered. Without data retention obligations, data that LEAs search for is likely to be gone (i.e. deleted or anonymised) when LEAs want to access it, thus rendering production orders and searches ineffective. Yet, the absence of data retention obligations may also push LEAs to collect more data early in the criminal investigation (or even proactively), to use more intrusive investigative techniques, to exploit police powers or to rely more heavily on data sharing with other authorities. To address the current situation appropriately, new EU legislation thus seems essential and urgently needed.

¹²⁷ Ibid., 314.

¹²⁸ Ibid., 315.

¹²⁹ Ibid., 310–311.

¹³⁰ Germany, Chapter 11, 295–296.

¹³¹ For an analysis of the national consequences of *Spacenet*, see S. Braun, 'German Data Retention Law Nullified, Again' (2023) 3 *European Data Protection Law Review* 353.

¹³² Germany, Chapter 11, 295.

¹³³ Ibid., 295.

¹³⁴ Ibid., 296.

¹³⁵ B. Vögel, 'La réception en Allemagne', Presentation at a research seminar (*Réceptions comparées de la jurisprudence européenne et l'accès aux données en procédure pénale*) organised by the University of Paris-Nanterre, Paris, 3 April 2023.

¹³⁶ Luxembourg, Chapter 13, 352.

16.4 DIGITAL EVIDENCE GATHERING AND COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

As explained, the cooperation of service providers is crucial today for gathering digital evidence in a criminal investigation. One should, however, note that this cooperation may be preceded or followed by, or interact closely with, investigative measures conducted by LEAs themselves. For instance, when a LEA wants to search a computer or an information system, it may require the cooperation of a service provider (or another private actor) to get access to the system. Or when a LEA seeks to intercept private communications of a suspect, it may be able itself to intercept part of those communications, while it relies on the intervention of a service provider for other communications. Finally, should a LEA need traffic or location data, it might order the production of such data by a service provider or, if the latter refuses to cooperate, decide to do a search and seizure at the premises of the service provider, this measure being clearly more intrusive and far-reaching. That is why the analysis of the cooperation of service providers should be ‘contextualised’ or embedded in a broader set of investigative measures aimed at gathering digital evidence.

In what follows, we will first discuss the issue of territorial scope and the distinction between domestic and cross-border collection of digital evidence (Section 16.4.1). Then we will focus more specifically on cooperation with service providers, drawing the distinction between mandatory and voluntary cooperation (Section 16.4.2). Subsequently, we will turn to a comparative analysis of how digital evidence is gathered in the different legal systems, both in a domestic and in a cross-border context (Sections 16.4.3 and 16.4.4). In doing so, special attention will be dedicated to cooperation with service providers.

16.4.1 *Territorial Scope: Domestic vs Cross-Border Gathering of Digital Evidence*

In the Westphalian system, which is the international legal order currently in place, national LEAs cannot execute any enforcement measures beyond their physical borders.¹³⁷ In other words, the physical borders limit their jurisdiction to enforce (contrary to the jurisdiction to prescribe, which is larger and may even be stretched to universal jurisdiction). Any act of enforcement undertaken on the territory of another country, however justified it may be, constitutes a violation of that country’s sovereignty and is hence illegal.¹³⁸

In contrast to these legal limitations, the flow of data in cyberspace knows no physical borders of that kind, except when countries (try to) limit access to cyberspace for users, which is the case for some non-democratic states.¹³⁹ Even within one country, data is processed and stored by a multitude of providers of online services which often have no physical presence, let alone an establishment or legal representative, in the country where their users are located and which, for technical and/or commercial reasons, store their users’ data in different locations around the world. Users often do not know where their data is stored. At EU level, the free flow of data has been facilitated by the internal market and, more specifically, by the EU’s digital services policy,

¹³⁷ See, e.g., M. Giacometti, *La récolte transfrontière de preuves électroniques dans le contexte européen* (Brussels: Bruylant/Larcier, 2023), 90–91.

¹³⁸ Permanent Court of International Justice on 7 September 1927 in the case of *SS Lotus*, Publications of the Permanent Court of International Justice, Series A-No. 70, 18–19; U. Sieber and C. Neubert, ‘Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty’ (2017) 20 *Max Planck Yearbook of United Nations Law Online*, 239. Also see, e.g., M. Corhay, ‘L’extension de la recherche dans un système informatique: Du droit belge à la Convention de Budapest sur la cybercriminalité’ (2020) 8 *Journal des tribunaux* 133–141.

¹³⁹ See Chapters 17 (China), 18 (Russia) and 19 (Turkey), this volume.

whose foundations were laid down in the 2001 e-Commerce Directive, seeking to minimise legal obstacles to electronic commerce by facilitating the establishment and provision of services by providers, tackling legal uncertainty and enhancing consumer confidence. Even if the regulation of digital services has become stricter in recent years (e.g. with the 2022 Digital Services Act) and notwithstanding the limitations imposed by the GDPR and the case law of the CJEU,¹⁴⁰ data still flows freely within the EU and, under certain conditions,¹⁴¹ across the EU's external borders. This situation obviously brings into question the Westphalian approach based on territoriality and creates major difficulties for LEAs willing to access data in the case of suspicion of criminal offences. Therefore, a crucial question is how to define enforcement jurisdiction in the digital era¹⁴² and, more specifically, how to distinguish between domestic and cross-border gathering of digital evidence, regarding both investigative measures undertaken by LEAs and cooperation with service providers.

Whereas the traditional territorial approach was based on the location of storage of the data and/or the location of the service provider's headquarters,¹⁴³ several of the analysed legal systems have moved away from a strictly territorial approach to facilitate cross-border data access by LEAs. Among the EU member states analysed in this book, some benefit from the presence of (several) global service providers or important data centres, while others do not have any major provider or data centre headquartered within their borders. For the former category, this permits a stronger focus on domestic measures (e.g. Luxembourg and Ireland),¹⁴⁴ while other states might have a strong incentive to develop rules extending domestic jurisdiction (e.g. Belgium and Germany).

Roughly speaking, one can distinguish three approaches to account for the challenges raised by cyberspace: remote searches and seizures by LEAs; 'domestication' of foreign service providers; and data localisation requirements.¹⁴⁵ Each of these approaches stretches to some extent the jurisdiction of national LEAs – a development that obviously did not take place without controversy.

For instance, a paramount example of 'domestication' is Belgium, which developed a new approach to construing territoriality with respect to foreign service providers: providers offering services on the Belgian market and targeting Belgian users are considered national providers, even without any physical presence on Belgian soil.¹⁴⁶ This approach clearly mirrors the interpretation of Article 18(1)(b) of the Cybercrime Convention concerning the production of subscriber information,¹⁴⁷ but applies to all data categories.¹⁴⁸

More recently, Germany, too, introduced such 'domestication' of foreign providers through a reform of the laws regulating the provision of telecommunication and telemedia services. Accordingly, foreign service providers falling into the scope of these laws must comply with law enforcement requests for content, traffic, usage and/or subscriber data without any involvement

¹⁴⁰ *Digital Rights Ireland*, para. 68.

¹⁴¹ GDPR, Art. 48.

¹⁴² For a more in-depth study of this question, see Chapter 2, this volume.

¹⁴³ *SS Lotus*; Sieber and Neubert, 'Transnational Criminal Investigations in Cyberspace'.

¹⁴⁴ Luxembourg, Chapter 13, 358.

¹⁴⁵ On the risks of data localisation laws, see, e.g., A. Chander and U.P. Lê, 'Data Nationalism' (2015) 64 *Emory Law Journal* 677, 730–733; J. Daskal and P. Swire, 'Why the CLOUD Act Is Good for Privacy and Human Rights', *Lawfare Blog*, 14 March 2018, www.lawfaremedia.org/article/why-cloud-act-good-privacy-and-human-rights.

¹⁴⁶ Belgium, Chapter 9, 232–234.

¹⁴⁷ See also Council of Europe, *T-CY Guidance Note #10: Production Orders for Subscriber Information (Article 18 Budapest Convention)*, 1 March 2017, 6.

¹⁴⁸ Franssen, 'The Belgian Internet Investigatory Powers Act', 539–41.

of foreign authorities.¹⁴⁹ This approach is not without controversy and has not yet been scrutinised by the German Constitutional Court.¹⁵⁰

16.4.2 *Nature of the Cooperation with Service Providers: Voluntary vs Mandatory*

When cooperating with service providers, LEAs in the selected EU countries resort to a mix of voluntary and mandatory cooperation. In general, one can observe, on the one hand, a tendency to use the mandatory instruments for national and EU providers and, on the other, a reliance on voluntary cooperation for obtaining data from US providers. Even if the latter have a local office in an EU member state, they are still bound by the limitations imposed by US law.¹⁵¹ Mandatory instruments (e.g. MLA requests or direct orders based on an international agreement) will therefore be necessary for obtaining content data. In contrast, other data may be provided on a voluntary basis thanks to the permissive nature of US law with respect to non-content data.

16.4.2.1 *Mandatory Cooperation*

The most important and overall prevalent type of cooperation is mandatory cooperation. Under this term we understand all situations where there is a legal basis for the order by the LEAs and service providers are compelled to react to the order by providing data or otherwise facilitating its acquisition. The sections that follow will analyse several mandatory cooperation duties in more detail. A common feature of these duties is that they are all reactive: a provider receives an order and is obliged to execute it.

16.4.2.2 *Voluntary Cooperation*

As has been observed elsewhere, ‘the distinction between voluntary and mandatory cooperation is not always easy to establish’.¹⁵² In this book, voluntary cooperation is understood as a form of cooperation where service providers are not under a legally enforceable obligation to respond to the requests coming from LEAs.¹⁵³ Cooperation is thus (largely) informal, even if it may be regulated to some extent, and it depends essentially on the service providers’ willingness to cooperate. As a result, this form of cooperation is characterised by a lack of legal certainty, which is unanimously regretted by LEAs¹⁵⁴ and which is detrimental for citizens whose data is requested.

Interestingly, none of the examined legal systems reported voluntary cooperation as forbidden. That said, one should not look for an express permission to cooperate. Rather, the possibility to cooperate on a voluntary basis results from the absence of a prohibition, as is the case in Germany,¹⁵⁵ Luxembourg¹⁵⁶ and Estonia,¹⁵⁷ where voluntary cooperation is sometimes used in the domestic context. In contrast, in Poland, voluntary cooperation is ‘very rare’: service providers

¹⁴⁹ Germany, Chapter 11, 299.

¹⁵⁰ Ibid., 299.

¹⁵¹ For further analysis of the US legal framework, see Chapter 21, this volume.

¹⁵² European Commission, Impact Assessment accompanying the Proposal for e-Evidence Regulation and the Proposal for e-Evidence Directive, SWD(2018) 118 final, 17 April 2018, p. 26 n. 37.

¹⁵³ Compare with *ibid.* (arguing that “voluntary” means that there is a domestic legal title which cannot be enforced directly in the recipient country”).

¹⁵⁴ See, e.g., *SIRIUS EU Digital Evidence Situation Report*, 28.

¹⁵⁵ Germany, Chapter 11, 299, 306.

¹⁵⁶ Luxembourg, Chapter 13, 365.

¹⁵⁷ Estonia, Chapter 10, 285.

are reluctant to cooperate when there is no legal basis for doing so because the production of data ‘may be treated as unauthorised violation of privacy’.¹⁵⁸

Voluntary cooperation seems to be used more frequently in the context of cross-border or international cooperation (see Section 16.4.4), for instance in Luxembourg,¹⁵⁹ or in Germany,¹⁶⁰ where it is considered rather an exception than the rule given the limits imposed by the GDPR as well as by the protection of the secrecy of electronic communications imposed by the e-Privacy Directive. Similarly, in Belgium, voluntary cooperation is essentially used in an international context¹⁶¹ and appears to be quite common with respect to non-content data.¹⁶² Even if, according to national law, data production requests addressed to foreign providers offering services on the Belgian market are considered legal orders, their enforceability raises fundamental questions from an international law perspective.¹⁶³

In Ireland, too, LEAs rely heavily on voluntary cooperation, even in a domestic context. The legal basis for such cooperation consists in disapplying the data protection restrictions on processing personal data. Until 2018 a clear, even if controversial, legal basis disapplying those restrictions if it was ‘required for the purpose of safeguarding the security of the State’ or ‘required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders ... [if] the application of those restrictions would be likely to prejudice [this enforcement]’.¹⁶⁴ This rule resulted in a thriving cooperation between LEAs and service providers on a voluntary basis. In any case, all major providers active in Ireland considered that they were allowed to provide non-content data on a voluntary basis and the use of this possibility was in line with the limitations stemming from US law. Hence, for instance, Facebook Ireland would provide non-content data on a voluntary basis but would require a mandatory instrument for content data. Since 2018, the legal situation has become less straightforward: section 41 of the 2018 Data Protection Act reflects the requirements of Articles 6 and 9 of the GDPR, insisting on the need for a specific legal basis for the transfer of data, and not just a mere disapplication of the prohibition to do so. Consequently, voluntary cooperation has become risky for service providers in Ireland.¹⁶⁵

As indicated, voluntary cooperation is usually characterised by the absence of a formalised legal procedure and strongly depends on the policy rules of service providers, which differ from one service provider to another, and which may change over time. Consequently, voluntary cooperation is not embedded in a clear protective legal framework.¹⁶⁶ The use of this type of cooperation creates a situation where a core public law function is outsourced to private authorities as the data controller is the one to determine whether the disclosure is necessary and proportionate.¹⁶⁷ Certain (mainly big) service providers have publicly stated that they check the proportionality of the LEA request and, if need be, limit the production of data to what in their view is proportionate.¹⁶⁸ This approach does not seem to be in

¹⁵⁸ Poland, Chapter 14, 387.

¹⁵⁹ Luxembourg, Chapter 13, 359, 365.

¹⁶⁰ Germany, Chapter 11, 299–300.

¹⁶¹ Belgium, Chapter 9, 251.

¹⁶² *Ibid.*, 255.

¹⁶³ *Ibid.*, 251–252.

¹⁶⁴ Section 8 of the 1988 and 2003 Irish Data Protection Acts.

¹⁶⁵ Ireland, Chapter 12, 325.

¹⁶⁶ See also J. Daskal, ‘Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues’ (2016) 8 *Journal of National Security Law & Policy* 473, 479.

¹⁶⁷ Ireland, Chapter 12, 323. See also S. Tosza, ‘Internet Service Providers as Law Enforcers and Adjudicators: A Public Role of Private Actors’ (2021) 43 *Computer Law & Security Review* 1–17.

¹⁶⁸ Belgium, Chapter 9, 255.

conformity with the requirements for access to data put forward in the CJEU's case law on data retention.¹⁶⁹

One potential limitation to the use of voluntary cooperation could result from the rules on admissibility of evidence. Yet, in most examined legal systems, data obtained through voluntary cooperation appears to be admissible.¹⁷⁰ In Ireland, for instance, evidence gathered that way is considered admissible in the same way as evidence gathered through mandatory cooperation.¹⁷¹ In Estonia, too, it is in principle admissible, unless it was gathered in violation of a fundamental right. Even in the case of such violation, exclusion of evidence is not automatic but requires checking the impact of the concrete violation.¹⁷² The same approach is applied in Luxembourg.¹⁷³ In Belgium, the mere violation of the right to privacy or data protection is not enough either; illegally obtained evidence is excluded only when the law explicitly provides nullity as a sanction (which is rarely the case), when the illegality affects the reliability of the evidence or when the use of the evidence violates the right to a fair trial.¹⁷⁴

16.4.3 Domestic Investigative Measures and Cooperation with Services Providers

As indicated, the collection of data for evidence purposes may be done by LEAs themselves or through cooperation with service providers. In some cases, there may be a combination of both (e.g. a search and seizure of data by LEAs after the service provider has given access to the information system or provided technical assistance). In the next subsections, we will take a closer look at domestic investigative measures and the cooperation duties of service providers.

16.4.3.1 Overview

16.4.3.1.1 PRODUCTION AND PRESERVATION ORDERS. A common go-to instrument at domestic level to acquire data held by service providers is the *production order*. Nevertheless, the scope of these orders varies across the different examined legal systems. Some legal systems provide for broad production orders requiring overall cooperation with LEAs, including the production of data, whereas others foresee specific production orders which relate to certain objects (in particular data) and/or to certain categories of persons. In certain member states, both types of order – general and specific – coexist.

First, an example of a general production order may be found in Ireland. This order targets not specifically digital evidence but more generally any document or any information that a person possesses (s. 15 of the Criminal Justice Act 2011).¹⁷⁵ Data falls into its scope, including content data.¹⁷⁶

An even more general provision is offered by Estonian legislation, where Article 215 of the Estonian Code of Criminal Procedure requires compliance with the orders and demands of

¹⁶⁹ See, e.g., *Digital Rights Ireland*, para. 61; *Tele2 Sverige*, para. 118.

¹⁷⁰ This corresponds to earlier research. See, e.g., European Commission, *Non-paper*, 5; SIRIUS EU Digital Evidence Situation Report, 37–38 (reporting that such evidence is admissible in court in seventeen out of twenty-three EU member states surveyed; exceptions are, e.g., the Czech Republic and Malta).

¹⁷¹ Ireland, Chapter 12, 326.

¹⁷² Estonia, Chapter 10, 276.

¹⁷³ K. Ligeti and S. Tosza, 'Admissibility of Evidence, Transnational E-Evidence and Fair-Trial Rights in Luxembourg', in L. Bachmaier Winter and F. Salimi (eds.), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights* (Oxford: Hart, 2024), 89–102, at 89.

¹⁷⁴ Belgium, Chapter 9, 224–225.

¹⁷⁵ Ireland, Chapter 12, 327–329.

¹⁷⁶ Ibid., 331.

competent authorities in criminal investigation. This very general provision can be used to order the expedited preservation or production of stored computer data.¹⁷⁷

In Germany, persons who are in possession of objects of interest to an investigation may be ordered to surrender those objects (§95(1) of the German Code of Criminal Procedure). This obligation extends to data.¹⁷⁸

Second, several legal systems offer examples of more specific production orders. For instance, Belgian law entails specific legal bases for producing data, distinguishing between identification/subscriber data (Art. 46bis of the Belgian Code of Criminal Procedure), traffic and location data (Art. 88bis of the same Code) and the content of communications (Art. 90quater of the same Code). The more sensitive the data, the more protective the procedural rules.¹⁷⁹ The secret nature of the measure (interception of content) triggers the highest procedural protection.¹⁸⁰

Similar provisions can be found in the Luxembourg Code of Criminal Procedure. Article 67-1 of this Code provides production orders for telecommunication services for traffic and location data.¹⁸¹ A similarly targeted order is provided in case of terrorist threats.¹⁸² Article 48-27 of the same Code provides for the production of subscriber data.¹⁸³

Polish law, too, contains specific production orders. These are addressed to, among others, post and telecommunications operators (Art. 218 §1 of the Polish Code of Criminal Procedure).¹⁸⁴

Some of those domestic production orders can also be used to (try to) compel foreign companies, which is provided by statutory law in Belgium,¹⁸⁵ and which is allowed by Irish case law.¹⁸⁶ In contrast, the aforementioned Estonian general provision is not applied to foreign providers offering services in Estonia.¹⁸⁷ In Poland, legally speaking, foreign service providers offering services in the territory could be addressed, but in practice the implementation of such orders appears problematic.¹⁸⁸

To the extent that production orders concern past data, their execution depends obviously on the availability of the data. This is where the discussion on data retention kicks in (see Section 16.3).

A production order may, of course, be preceded by a *preservation order* (sometimes called a ‘quick freeze’¹⁸⁹). For instance, in Estonia, the aforementioned Article 215 of the Estonian Code of Criminal Procedure, which requires compliance with the orders and demands of competent authorities in criminal investigations, may be used to order expedited preservation of stored computer data.¹⁹⁰

The Luxembourg Code of Criminal Procedure entails a rapid preservation measure in Article 48-25, which was added to the Code in 2014 by a law implementing the Budapest Convention. It

¹⁷⁷ Estonia, Chapter 10, 265.

¹⁷⁸ Germany, Chapter 11, 301.

¹⁷⁹ Belgium, Chapter 9, 238–241.

¹⁸⁰ *Ibid.*, 243–244.

¹⁸¹ Luxembourg, Chapter 13, 360–361.

¹⁸² *Ibid.*, 462.

¹⁸³ *Ibid.*, 356.

¹⁸⁴ Poland, Chapter 14, 374. S. Tosza, and S. Steinborn, ‘Poland’, in U. Sieber, T. Tropina and N. von zur Mühlen (eds.), *Access to Telecommunication Data in Criminal Justice* (Berlin: Duncker & Humblot, 2021), 1167–1220.

¹⁸⁵ Belgium, Chapter 9, 251.

¹⁸⁶ Ireland, Chapter 12, 332.

¹⁸⁷ Estonia, Chapter 10, 265.

¹⁸⁸ Poland, Chapter 14, 384.

¹⁸⁹ See, e.g., Luxembourg, Chapter 13, 360.

¹⁹⁰ Estonia, Chapter 10, 265.

seems to go beyond the requirements of the Convention, however, by extending this quick freeze provision not only to traffic data but to any type of data, including content data.¹⁹¹ A similarly extensive quick preservation provision is laid down in the Belgian Code of Criminal Procedure since 2016.¹⁹² To the contrary, expedited preservation of data is still missing in the Irish law.¹⁹³

16.4.3.1.2 SEARCHES. Another legal possibility for gathering digital evidence is a *search*. Like for production orders, one may distinguish between general search provisions and more specific legal bases. For instance, in Germany, the main way of acquiring electronic evidence is to perform a search (according to §§102 ff of the German Code of Criminal Procedure) and to seize storage devices.¹⁹⁴ In Luxembourg, too, the general search provision is used, even if it may be accompanied with specific technological provisions, such as the duty of cooperation for persons having specific knowledge of the IT system, in order to facilitate the search of the device.¹⁹⁵ And under Estonian law, the general provisions on searches (excluding ‘places where the investigator could only step on virtually’,¹⁹⁶ thus excluding remote searches of information systems) and inspections are used.¹⁹⁷

Examples of specific search provisions can be found in Belgium and Spain. The Belgian Code of Criminal Procedure offers provisions on network searches, which may also potentially be extended to another information system, and also contains provisions on cooperation duties (e.g. obligation to provide information on the accessibility and operation of the information system).¹⁹⁸

In Ireland, remote or extended searches are possible, too. A search warrant is understood as permitting access to a computer to which a computer being searched is connected. Thus, if a webmail service is hosted abroad but the computer that is searched permits access to it, this webmail service can also be searched.¹⁹⁹

The possibility to extend a search is also accepted in Germany. However, it is so far not clear if a search may extend beyond national borders, even if German authorities seem to be willing to be less stringent in their efforts to verify where the data in question is located.²⁰⁰

Under Spanish law, a search can be extended to another ‘non-specified’ device ‘provided that the required data is lawfully accessible through the initial electronic system, and it is easily available’.²⁰¹ This potentially extends beyond national borders, even if there is no case law yet on this matter.²⁰²

In Belgium, the law explicitly permits cross-border remote searches, on the condition that the foreign state is notified if it can be reasonably identified. However, in practice, such notification is hardly ever made.²⁰³

¹⁹¹ Luxembourg, Chapter 13, 360.

¹⁹² Belgium, Chapter 9, 246.

¹⁹³ Ireland, Chapter 12, 329.

¹⁹⁴ Germany, Chapter 11, 290.

¹⁹⁵ Luxembourg, Chapter 13, 364.

¹⁹⁶ Estonia, Chapter 10, 265.

¹⁹⁷ Ibid., 265–266.

¹⁹⁸ Belgium, Chapter 9, 241.

¹⁹⁹ Ireland, Chapter 12, 331.

²⁰⁰ Germany, Chapter 11, 292.

²⁰¹ Spain, Chapter 15, 414.

²⁰² Ibid., 416.

²⁰³ Belgium, Chapter 9, 231.

16.4.3.1.3 INTERCEPTION. Finally, *interception* of data is another useful investigation measure that can be conducted by LEAs themselves but may also encompass duties for providers to facilitate or enable the interception. Such duties are embedded, for instance, in Articles 20(1)(b) and 21(1)(b) of the Cybercrime Convention.

For instance, the Luxembourg Code of Criminal Procedure contains a series of specific measures for that purpose which are applicable to all types of data and require mandatory cooperation of service providers.²⁰⁴ Similar provisions can be found in the German²⁰⁵ and Estonian legal systems.²⁰⁶ The Irish legal system, too, contains such a possibility, which is based on interception warrants. The latter are, however, limited to ‘essentially traditional telecoms and connectivity providers but [not applicable to] e.g. over-the-top communication services, webmail providers, or other information society services’.²⁰⁷

16.4.3.2 Legal Conditions

On top of the variety of measures, legal systems seem to vary considerably with respect to the applicable legal conditions. Nevertheless, a few common conditions come to the fore.

Among the criteria used to assess whether a measure can be applied, a crucial one is proportionality.²⁰⁸ Application of measures may be limited to certain categories of offences, which may be enumerated²⁰⁹ or may require a certain penalty threshold. For instance, in Ireland, search and production orders are limited to the investigation of offences carrying a possible five-year prison sentence.²¹⁰ In comparison to this threshold, the European Production Order will be available to a longer list of offences than this domestic instrument, as the limitation provided for by the e-Evidence Regulation (and just as regards content and traffic data) is of three years only.²¹¹

Orders, such as production orders, shall generally take a written form,²¹² but exceptions are possible. For instance, an exception to this rule can also be found in Estonia, where a request to an electronic communications provider for subscriber information can be submitted orally.²¹³ In Belgium, the production of subscriber and traffic data may be ordered orally in urgent cases, provided that the order is confirmed in writing as soon as possible (Art. 46bis, §1, para. 5 and 88bis, §1, last para. of the Belgian Code of Criminal Procedure).

Interestingly, despite the privacy-sensitive nature of certain orders, a judicial warrant may not always be necessary. For instance, the aforementioned general production order in Germany, which concerns any type of data, is considered to not require a judicial warrant in practice. Nevertheless, it is interesting to note that such a warrant will often be issued . . . at the request of the provider.²¹⁴ A similar situation has been described for Spain, although especially in the context of voluntary cooperation.²¹⁵

²⁰⁴ Luxembourg, Chapter 13, 364.

²⁰⁵ Germany, Chapter 11, 302.

²⁰⁶ Estonia, Chapter 10, 274–275.

²⁰⁷ Ireland, Chapter 12, 327–329.

²⁰⁸ Germany, Chapter 11, 301; Belgium, Chapter 9, 237; Spain, Chapter 15, 406.

²⁰⁹ Estonia, Chapter 10, 274.

²¹⁰ Ireland, Chapter 12, 327–329.

²¹¹ E-Evidence Regulation, Art. 5(4).

²¹² For example, Belgium, Chapter 9, 238–240.

²¹³ Estonia, Chapter 10, 273.

²¹⁴ Germany, Chapter 11, 302.

²¹⁵ Spain, Chapter 15, 413–414.

16.4.3.3 Some Specific Cooperation Duties for Service Providers

In addition to the foregoing measures and cooperation duties, it is worthwhile focusing on three specific duties for service providers – or a notable lack thereof – which are often discussed (and criticised) in the context of digital evidence gathering:

- (1) duty to decrypt;
- (2) duty to adapt technology to allow certain procedural measures (e.g. duty to create an interception capability);
- (3) duty to ensure confidentiality on the undertaken measure.

These duties can be found in several of the examined legal systems, even if some grey areas remain.

Examples of the first two duties can be found in Belgian law, partly codified in legal provisions and partly developed or extended through case law.²¹⁶ Service providers can be ordered to give access to an information system (Art. 88quater of the Belgian Code of Criminal Procedure) and to make content accessible in the context of an interception measure (Art. 90quater of the same Code). In the *Skype* case, the Court of Appeals ruled that the company had an obligation to cooperate and should have taken the necessary technical measures to do so (in particular, by providing for an interception capability, despite the facts that communications through Skype are end-to-end encrypted and there is a lack of any technical infrastructure in Belgium); the Supreme Court did not rule explicitly on this matter and thus it remains unclear to what extent such duty exists.²¹⁷

In Ireland, as information must be provided in a form that is legible, the cooperation duties may extend to handing over a password or otherwise enabling the examination of data, including by removing encryption applied by the provider (s. 15(6) of the Criminal Justice Act 2011). This obligation is, however, limited to situations where the provider holds the key on behalf of the user; there shall be no obligation to decrypt or provide a back-door solution if the key is held by the user.²¹⁸

The duty to adapt the used technology and, if necessary, remove encryption can also be found in German law, and the validity of those provisions with the Basic Law was confirmed by the German Federal Constitutional Court.²¹⁹ However, a production order does not automatically entail an obligation to decrypt. Nevertheless, a stored password or key to decrypt can be obtained by means of a production order. Furthermore, a person who is not a suspect may be questioned as a witness as regards such password or key. For those reasons, service providers generally cooperate in decryption on a voluntary basis, to avoid being called in that capacity.²²⁰

Such obligation may also be found in the Spanish legal order, as resulting from the general duty of cooperation stemming from the Spanish Constitution (Art. 118) and from more specific legal provisions in the Spanish Code of Criminal Procedure and sectoral laws.²²¹ Similarly, in Luxembourg, an investigating judge may order a person (except the suspect) with special knowledge of the IT system or service to decrypt or otherwise provide access to seized data.²²²

²¹⁶ Belgium, Chapter 9, 234 and 243.

²¹⁷ V. Franssen and M. Corhay, 'La fin de la saga Skype: Les fournisseurs de services étrangers obligés de collaborer avec la justice belge en dépit des possibilités techniques et de leurs obligations en droit étranger' (2019) 8 *Revue de droit commercial belge* 1016–1019.

²¹⁸ Ireland, Chapter 12, 330.

²¹⁹ German Federal Constitutional Court, 2 BvR 2377/16; Germany, Chapter 11, 302.

²²⁰ Germany, Chapter 11, 301.

²²¹ Spain, Chapter 15, 418.

²²² Luxembourg, Chapter 13, 362.

To the contrary, Estonia does not oblige its service providers to decrypt; in fact, enlisting the assistance of private actors in breaking into an encrypted storage device might render the evidence inadmissible.²²³

As to the third duty mentioned above, service providers may also be obliged to keep silence on applied measures and data transfers. In the examined national systems, several examples of confidentiality obligation are encountered.

For instance, German law provides an obligation for telemedia service providers to keep secret the requests addressed to them.²²⁴ In Luxembourg, too, persons providing help to the investigation are under an obligation of confidentiality.²²⁵ So must service providers in Belgium – and by extension any person who is at some point involved in the investigation – keep secret the investigation measure and their own involvement in the investigation. This duty is not limited in time or based on a concrete assessment; it must be complied with throughout the whole criminal investigation, which is regarded as secret. Violation of this duty is a criminal offence.²²⁶ In contrast, in the absence of a notification duty for LEAs under national law, service providers (especially global and US-based service providers) tend to inform their users as per their policies, unless it is outright forbidden by law.²²⁷

16.4.3.4 Enforcement Mechanisms

Typically, national legal systems provide for sanctions for non-compliance with the cooperation duties described just now. However, both the nature and the level of severity of those sanctions vary. So does their personal scope of application as they may focus only on the service providers as legal persons or also target their employees (i.e. natural persons) who are responsible for cooperation with LEAs.

The consequences of non-compliance that legal systems most frequently provide for are pecuniary fines, although their level of severity differs significantly. In some member states the fines may be relatively small, which raises the question whether they can have an effective compelling effect. For instance, Luxembourg punishes non-compliance with production orders with a fine of only 100 to 5,000 euros.²²⁸ Similarly, in Germany, non-compliance with a lawful request made by the authorities is punished with a fine of up to 1,000 euros.²²⁹ In Estonia, violation of the obligation to preserve subscriber and communications data is punishable for legal persons with a fine of up to 3,200 euros. A similar sanction is foreseen for violations of

²²³ Estonia, Chapter 10, 275–276.

²²⁴ Germany, Chapter 11, 302–303.

²²⁵ Luxembourg, Chapter 13, 361.

²²⁶ Belgium, Chapter 9, 247.

²²⁷ Ireland, Chapter 12, 322. Whether the absence of such notification is in conformity with the EU legal framework on data protection, in particular the Law Enforcement Directive and the data subject's right to information (Art. 13), is questionable, notwithstanding that specific nature of criminal investigations. Even if the Law Enforcement Directive allows for certain restrictions (e.g. Art. 13(3)(b)) – and so does Article 23(1)(d) GDPR with respect to data processed by service providers – those restrictions should not curtail the essence of the data subject's rights. Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89 (Law Enforcement Directive). See, e.g., V. Franssen and M. Corhay, 'Commentary on Article 18 LED', in E. Kosta and F. Boehm (eds.), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford: Oxford University Press, 2024).

²²⁸ Luxembourg, Chapter 13, 361.

²²⁹ Germany, Chapter 11, 299–300.

obligations to preserve documentation (logs or applications) by electronic communication undertakings in relation to surveillance activities conducted by authorities.

Much higher sanctions are provided by Luxembourg law for failure to comply with law enforcement requests in terrorist cases, where fines can go up to 125,000 euros, and similarly in the case of (relatively rarely used) orders to intercept data.²³⁰ In Belgium, failure to comply with production orders was punished with a fine of 208 to 80,000 euros at the time of writing the national chapter; very recently, the fine level has been further increased to 800–240,000 euros. Non-cooperation with other measures may increase these fines applicable to legal persons to an even higher level, that is, to 24,000–576,000 euros in the context of searches of an IT system or network searches, when the offender is a legal person.²³¹ Even harsher fines can be used in Spain for providers which fail to comply with cooperation duties: fines can range from 50,000 to 20,000,000 euros and also offer the possibility to impose disqualification of up to five years for service providers, which results in preventing them from offering services in relation to any networks or the provision of electronic communication services in that period.²³²

Several legal systems also offer the possibility to punish natural persons not only with fines but including with deprivation of liberty. For instance, in Germany, non-compliance with cooperation duties may lead to a detention of up to six months.²³³ Belgium also offers such possibilities for non-compliance, inter alia, in the context of a search of an IT system or a network search, where imprisonment can go even up to five years.²³⁴

Nevertheless, in a few instances, non-cooperation does not result in the possibility of imposing sanctions. For instance, non-fulfilment of data retention duties in Ireland is reported to not carry a risk of any sanction.²³⁵ Sanctions may also be more difficult to enforce, in particular in the context of ‘domestication’ of foreign providers, as reported in Germany²³⁶ and in Belgium.²³⁷

Some legal orders may also offer a possibility to justify or excuse non-compliance. This is the case for Ireland, where even when there is a possibility to impose fines, this may be avoided if there is a reasonable excuse. It is not clear whether this term, which is not defined in the law, may include such reasons as potentially high costs or conflicting legal obligations.²³⁸ In other jurisdictions, the case law remains inconclusive on the possibility to invoke a conflicting legal obligation under foreign law, as is illustrated by the Belgian *Yahoo!* case and the Belgian–Luxembourg *Skype* case.²³⁹

Finally, sanctions may also be foreseen for violations of privacy. Such negative consequences may potentially put pressure on service providers when they receive requests (especially based on voluntary cooperation) that do not seem to be well founded. In Luxembourg, for instance, imprisonment may go up to three years for breaches of confidentiality and may be cumulated with fines.²⁴⁰

This divergence of approaches to sanctions is highly relevant from the perspective of the e-Evidence Regulation. Article 15(1) of the Regulation leaves it to the member states to design the enforcement system. It provides that they ‘shall lay down rules on pecuniary penalties applicable to [relevant] infringements . . . and shall take all measures necessary to ensure that they are

²³⁰ Luxembourg, Chapter 13, 362.

²³¹ Belgium, Chapter 9, 238–240.

²³² Spain, Chapter 15, 418.

²³³ Germany, Chapter 11, 299–300.

²³⁴ Belgium, Chapter 9, 238–240.

²³⁵ Ireland, Chapter 12, 322–323.

²³⁶ Germany, Chapter 11, 300.

²³⁷ Belgium, Chapter 9, 251–252.

²³⁸ Ireland, Chapter 12, 323.

²³⁹ Belgium, Chapter 9, 236; Franssen and Corhay, ‘La fin de la saga Skype’, 1020–1021.

²⁴⁰ Luxembourg, Chapter 13, 362.

implemented. The pecuniary penalties provided for shall be effective, proportionate and dissuasive.’ As we can conclude from the above-presented panorama, member states seem to have a very different understanding of what effective, proportionate and dissuasive may mean in that context. Furthermore, the last sentence of Article 15(1) requests member states to ensure ‘that pecuniary penalties of up to 2% of the total worldwide annual turnover of the service provider’s preceding financial year can be imposed’. This provision imposes quite a significant departure from the practice of states, which foresee relatively small sanctions. It will be of paramount significance to the efficacy of the new European Production Orders what kinds of sanctions member states effectively provide for and at which level of severity they are ready to impose them in practice.

16.4.3.5 Legal Remedies

Given the intrusive character (albeit of varied degree) of the above-analysed measures, legal remedies for the persons concerned are of key importance. While the right to an effective legal remedy is a key aspect of the right to a fair trial, neither the European Convention on Human Rights nor the Charter on Fundamental Rights of the EU specifies the form that such remedy should take. Therefore, the type of legal remedy as well as the stage at which and the conditions on which it may be exercised may differ a lot across EU member states. In some cases, the person may have a direct legal remedy against the investigative measure; in others (more commonly), the person will be able to resort only to a more general legal remedy or oppose the use of the collected evidence. In addition, one may wonder whether there could be instances in which the service provider, too, should be able to exercise a legal remedy to the benefit of its customers/users.

It is noteworthy that the authors of several national chapters point out deficiencies regarding the legal protection offered to those persons.²⁴¹ On the one hand, there might be lack of legal protection, particularly in the case of voluntary cooperation. This is especially problematic if LEAs strongly rely on the data acquired that way.²⁴² Indeed, the CJEU has ruled, in the context of data retention, that data obtained in violation of EU law (including the right to respect for private life and the right to protection of personal data, Articles 7 and 8, respectively, of the EU Charter) should under certain conditions be excluded as evidence, including when it ‘is likely to have a preponderant influence on the finding of facts’.²⁴³ On the other hand, even if a protective legal framework exists, its use and effectiveness may be limited by existing rules.²⁴⁴

Besides the need for *ex ante* judicial authorisation in the case of some (but not all) of the measures examined earlier, legal orders generally offer the right to review the measure according to which data affecting the person concerned was gathered. That is the case, for instance, in Germany,²⁴⁵ Ireland²⁴⁶ and Poland.²⁴⁷ In Luxembourg, too, a person concerned may request nullity of an act of a preliminary investigation or judicial inquiry.²⁴⁸

An important limitation to the effectiveness of remedies may result from withholding information about the measure from the person concerned. Not only there may be no legal obligation

²⁴¹ See, e.g., Belgium, Chapter 9, 250–251; Ireland, Chapter 12, 332–333 and 334–336; Poland, Chapter 14, 389.

²⁴² Ireland, Chapter 12, 334–335.

²⁴³ See, e.g., *La Quadrature du Net*, paras. 226–227.

²⁴⁴ For example, Luxembourg, Chapter 13, 363.

²⁴⁵ Right to legal review is enshrined in Art. 19(3) of the German Basic Law; Germany, Chapter 11, 304.

²⁴⁶ Ireland, Chapter 12, 333.

²⁴⁷ Polish Code of Criminal Procedure, Art. 236 §1; Poland, Chapter 14, 389.

²⁴⁸ Luxembourg, Chapter 13, 363.

under national law to inform the data subject about the transfer of his/her data to law enforcement authorities, like in Belgium or Ireland,²⁴⁹ but, as already mentioned (Section 16.4.3.3), service providers may also be under a secrecy obligation, in which case the person in question will not know about the measure, and – logically – will not be able to oppose or complain about it. Unless the secrecy is lifted (e.g. when access to the case file is granted at some point of the investigation), that person will be able to question the measure only in the course of the trial or, at best, at the end of the investigation. But that right may also be curtailed by very short time limits for the filing of a complaint, as is the case in Luxembourg.²⁵⁰

Another moment of control of the lawfulness of gathering electronic evidence is during trial,²⁵¹ when thus gathered evidence may be excluded as inadmissible. That is the case, for instance, in Spain.²⁵² However, with respect to the admissibility of illegally obtained evidence, significant diversity of approaches exists in the EU with different consequences attached to violations of procedural measures.²⁵³ Even if evidence is gathered in violation of the law, it is not always automatically excluded. For instance, in Estonia, a violation committed while executing a measure does not inevitably lead to the exclusion of the measure; such an effect is reserved only for violations committed in the process of obtaining a warrant for the measure in question.²⁵⁴ Furthermore, at that point it might not be possible to question the validity of evidence anymore if the options that existed earlier were not used. That is the case in Luxembourg, where the so-called *purge de nullité* results in illegally or improperly obtained evidence becoming valid if not questioned at the latest within five days from the moment the investigating judge charged the accused with a criminal offence.²⁵⁵

Finally, it is important to mention the limitation to the use of digital evidence covered by a legal privilege, such as the client–attorney privilege or journalists’ source protection.²⁵⁶ Those protective rules are, however, not absolute. For instance, in Estonia, information can be used if it was already disclosed or if the privilege was evidently misused.²⁵⁷ Belgian law does not contain any protection for privileged information which is stored using an online service not by the professional in question (such as an attorney or a medical doctor) but by the client or patient.²⁵⁸ Protection is also lacking in Ireland in the context of the 1993 Interception of Postal Packets and Telecommunications Messages (Regulation) Act, which allows ‘interception of journalists’ communications without prior judicial authorisation, contrary to the standards established by the ECtHR’.²⁵⁹

16.4.4 Cross-Border Investigative Measures and Cooperation with Service Providers

Once it is established that a situation is cross-border in nature (e.g. due to the implication of a foreign service provider), a distinction must be made between two possible scenarios. Either the cooperation involves a competent authority of the other (requested) country (i.e. indirect access or mediated cooperation) or cooperation consists in LEAs sending their requests directly

²⁴⁹ For example, Belgium, Chapter 9, 246–247; Ireland, Chapter 12, 333.

²⁵⁰ Luxembourg, Chapter 13, 369.

²⁵¹ In some jurisdictions, this issue may also be raised at a pre-trial hearing. For example in Belgium, in the case of a judicial inquiry (Belgian Code of Criminal Procedure, Art. 131).

²⁵² Spain, Chapter 15, 421.

²⁵³ L. Bachmaier Winter and F. Salimi (eds.), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights* (Oxford: Hart, 2024).

²⁵⁴ Estonia, Chapter 10, 276.

²⁵⁵ Ligeti and Tosza, ‘Admissibility of Evidence’, 97.

²⁵⁶ See, e.g., Germany, Chapter 11, 290.

²⁵⁷ Estonia, Chapter 10, 277.

²⁵⁸ Belgium, Chapter 9, 251.

²⁵⁹ Ireland, Chapter 12, 334.

to foreign service providers, without any intervention of a public authority of the state where the service provider is located (i.e. direct cooperation or unmediated access).²⁶⁰

Mediated access is based on legal instruments of transnational or international cooperation between sovereign states, which entail MLA provisions. Examples of such legal instruments are the European Convention on Mutual Assistance in Criminal Matters²⁶¹ and the Cybercrime Convention. In addition to multilateral treaties, bilateral MLA agreements may exist. At EU level, mediated cooperation is based on the principle of mutual recognition, with the European Investigation Order (EIO) Directive²⁶² as prime example.

Among the relevant international instruments, the EU countries selected for this study have all adopted and ratified the UN Convention against Transnational Organized Crime²⁶³ as well as the European Convention on Mutual Assistance in Criminal Matters, together with its First²⁶⁴ and Second Additional Protocols. As to the Council of Europe Convention on Cybercrime, all examined countries signed and ratified it, with the notable exception of Ireland, which signed the Convention but failed to ratify it. Its First Additional Protocol²⁶⁵ was signed and ratified by Germany, Luxembourg, Poland and Spain. However, Belgium and Estonia failed to ratify it, while Ireland has not even signed that Protocol. The Second Additional Protocol has already been signed by all selected countries, except for Ireland and Poland. That said, the other five countries have yet to ratify this Protocol, which can be explained, though, by the recent adoption of the instrument and the parallel legislative work at EU level.²⁶⁶

At EU level, the EIO is a key instrument for cross-border gathering of (any type of) evidence, involving close cooperation between the judicial authorities of the issuing state and those of the executing state. Nevertheless, once again, Ireland is not part of that instrument as it decided not to opt in (at least so far), considering that the text was ‘inconsistent with Irish law and practice’.²⁶⁷

Joint investigation teams (JITs), which can be established on the basis of Article 13 of the EU MLA Convention, constitute another option enabling cross-border collection of evidence. In recent years, they have been used to crack the encrypted communication tools of criminal organisations.²⁶⁸ It is likely that JITs will be used more often in the future for gathering digital evidence, as they allow the police authorities of different states to join forces and share knowledge and best practices. Moreover, with Article 12 of the Second Additional Protocol to

²⁶⁰ S. Carrera, G. González Fuster, E. Guild and V. Mitsilegas, *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights*, Centre for European and Policy Studies (Brussels: Centre for European Policy Studies (CEPS), 2015), 6.

²⁶¹ Council of Europe, European Convention on Mutual Assistance in Criminal Matters, ETS No. 030, www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=030.

²⁶² Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (EIO Directive) [2014] OJ L130/1.

²⁶³ United Nations Convention against Transnational Organized Crime, adopted by resolution 55/25 of 15 November 2000, https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=en.

²⁶⁴ Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, ETS No. 099, www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=099.

²⁶⁵ Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty=189.

²⁶⁶ At the moment of finalising this chapter – December 2023 – the Protocol has already gathered forty-one signatures; however, only two countries have ratified it so far.

²⁶⁷ Ireland, Chapter 12, 336.

²⁶⁸ J.-J. Oerlemans and S. Royer, ‘The Future of Data-Driven Investigations in Light of the Sky ECC Operation’ (2023) 14(4) *New Journal of European Criminal Law* 434–458; J.-J. Oerlemans and D. van Toor, ‘Legal Aspects of the EncroChat Operation: A Human Rights Perspective’ (2022) 30(3–4) *European Journal of Crime, Criminal Law and Criminal Justice* 309–328.

the Cybercrime Convention also providing for a legal basis for JITs, this tool will become available at a larger scale, in cooperation with other Council of Europe states and even non-Council of Europe states to the extent that they will have ratified the Second Additional Protocol.

Contrary to indirect cooperation, direct cooperation does not yet have a legal basis. It is based on the voluntary collaboration of the service provider and only possible to the extent that it is not explicitly forbidden (see Section 16.4.2.2). Direct compulsory cooperation would constitute a violation of international law. For instance, in Germany, any request that is accompanied by a threat of any enforcement measure or detrimental consequence is considered illegal, unless allowed by international law (No. 121 [4] lit. a of the Guidelines for Foreign Relations in Criminal Affairs).²⁶⁹ Often, voluntary cooperation is highly informal and thus not based on detailed rules.²⁷⁰ This does not, however, mean that there is no need for a legal basis on which to issue requests based on voluntary cooperation. For instance, in Germany, the request must be in conformity with the constitutional requirement of a legal basis to collect personal data.²⁷¹ Therefore, authorities shall use the same legal basis as when collecting data within Germany by a compelling order and respect its conditions and procedural requirements. In Luxembourg, too, despite (or because of) the lack of a legal framework, the conditions applicable to the measure in the domestic context would also need to be complied with.²⁷² As will be shown in Section 16.4.4.2, this type of cooperation among EU member states is limited in particular by the exigencies of the GDPR.

At international and EU levels, the lack of a legal framework for direct cooperation will change in the coming years due to two new legal instruments that will create the possibility for issuing direct cross-border orders to foreign service providers. These instruments are the Second Additional Protocol to the Cybercrime Convention and the e-Evidence Regulation.²⁷³

In what follows, we will first discuss whether and how the seven selected EU member states deal with the cooperation of their LEAs with foreign service providers (Section 16.4.4.1). We will then reverse the perspective and analyse whether national law authorises (or condones) the cooperation of domestic service providers with foreign LEAs or whether it contains a so-called blocking statute (Section 16.4.4.2).

16.4.4.1 Cooperation of National LEAs with Foreign Service Providers

As explained, mediated access or indirect cooperation is based on international and European MLA instruments and national law implementing those instruments. These instruments constitute an incomplete and partially overlapping patchwork. Therefore, the preliminary question as to which instrument is (most) applicable may not be easy to answer. As to unmediated or direct cooperation, under the Westphalian system, it can only be voluntary; otherwise, it would be considered to violate the sovereignty of another country and thus the collected evidence should, in principle, not be admissible at the subsequent trial.²⁷⁴ At least, that is the theory . . .

The problem is that states often ‘domesticate’ cross-border situations, thus treating them like purely internal situations (see Section 16.4.1). Earlier research also shows that the criteria used by

²⁶⁹ Germany, Chapter 11, 305.

²⁷⁰ For example, Luxembourg, Chapter 13, 369–370; Estonia, Chapter 10, 285.

²⁷¹ Germany, Chapter 11, 306.

²⁷² Luxembourg, Chapter 13, 366.

²⁷³ For detailed analysis of these instruments, see Chapters 7 and 8, this volume.

²⁷⁴ Germany, Chapter 11, 306. German Federal Court of Justice, Order of 2 March 2022, 5 StR 457/21, mn. 33.

member states to distinguish between domestic and foreign providers ‘vary significantly’.²⁷⁵ To the extent that states do label a situation ‘cross-border’, direct cooperation seems limited to voluntary cooperation, with all the uncertainties it brings.

In certain selected countries, such as Estonia, direct mandatory cooperation with foreign service providers is excluded as there is no legal basis in the Estonian Code of Criminal Procedure to oblige such providers to comply with orders from Estonian LEAs.²⁷⁶ In Germany, as indicated, the Constitution requires a legal basis for collecting personal data.²⁷⁷ In addition to the national legal basis for data collection, an important role for guaranteeing the legality of voluntary cooperation between the German authorities and US service providers is the ‘General Permission Letter’ issued by the US Department of Justice, which concerns the disclosure of traffic and subscriber data.²⁷⁸

When voluntary cooperation is not possible (in particular with respect to content data), the only admitted way to achieve cross-border gathering of digital evidence is to issue an EIO or an MLA request.²⁷⁹ This comes back in most national chapters (see later in this section).

It is very difficult to establish the practice in that respect as official statistics are lacking and stakeholders are reluctant to disclose detailed information.²⁸⁰ While the transparency reports of the big (mainly US-based) service providers offer some insight, they do not make a distinction between mandatory and voluntary direct cooperation.²⁸¹ When added to the blurred distinction at national level – for instance Belgium – between mandatory and voluntary production ‘orders’, it is hard to get a clear view on the situation.

Overall, the national chapters confirm that the scope of direct voluntary cooperation with US providers is limited to non-content data (e.g. name, email address, date of birth, telephone number and registration IP address, timestamps, recent IP addresses and network connections),²⁸² while content data should be disclosed only upon a processed MLA request. The latter results from the US blocking provision, which allows US-based service providers to disclose non-content data directly to foreign service providers but forbids the disclosure of content data. This blocking provision may be disapplied with countries that sign the agreement with the US based on the CLOUD Act. Such agreements have already been adopted with the UK and Australia.²⁸³ The EU and the US have the ambition to reach a similar agreement. Whereas these negotiations with the EU, mandated by the Council,²⁸⁴ were long stalled until an interinstitutional agreement on the e-Evidence package was reached, they have resumed since March 2023 but are still ongoing at the time of finalising this chapter.

Even if disclosure of certain types of data to EU law enforcement authorities is already allowed, it was noted, for example in the case of Luxembourg, that not all service providers agree to cooperate in an unmediated manner.²⁸⁵ Interestingly, Belgium seems to have a higher

²⁷⁵ European Commission, *Non-paper*, at 4.

²⁷⁶ Estonia, Chapter 10, 285.

²⁷⁷ Germany, Chapter 11, 306.

²⁷⁸ *Ibid.*, 306.

²⁷⁹ Estonia, Chapter 10, 286; Poland, Chapter 14, 17, 391.

²⁸⁰ See, e.g., Luxembourg, Chapter 13, 365; Germany, Chapter 11, 306.

²⁸¹ Belgium, Chapter 9, 255.

²⁸² Luxembourg, Chapter 13, 367.

²⁸³ For more details, see Chapter 21 on the US, this volume.

²⁸⁴ European Council, Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 9114/19, 21 May 2019.

²⁸⁵ Luxembourg, Chapter 13, 267.

success rate of direct requests.²⁸⁶ The success can be explained by the existence of a (well-functioning) single point of contact (SPoC) at the level of national LEAs.²⁸⁷ The creation of such a SPoC is an obligation under Article 35 of the Cybercrime Convention and aimed to facilitate the collection of digital evidence and mutual assistance (i.e. mediated access). In practice, service providers perceive SPoCs as ‘quality filters’ for data requests.²⁸⁸ Under the Second Additional Protocol, the role of these SPoCs will increase, notably in the context of expedited disclosure of stored data in an emergency (Art. 9).

A more extensive practice of providing non-content data appears to exist in Ireland among US service providers that are established there for the purpose of their operations in the EU. While detailed information is not available, this practice was revealed during a 2011 audit of Facebook Ireland by the Data Protection Commissioner. Facebook considered that such disclosures were permitted based on users’ consent and their own – arguably incorrect – interpretation of the Irish law.²⁸⁹ The application of consent-based transfer was already questionable under previous EU legal framework,²⁹⁰ but since the entering into force of the GDPR it is even more so under its Article 7.²⁹¹ Not surprisingly, research into Irish law and practice highlights a lack both of transparency and of fundamental rights safeguards to prevent abuse.²⁹²

As regards legal remedies, the mere fact that the data is obtained through direct cooperation with a foreign service provider cannot be challenged, for instance, in Luxembourg. Only the investigative measure in the course of which cooperation is undertaken may be questioned according to the rules applicable to that measure.²⁹³ The approach may be similar for indirect cooperation, although the cooperation instrument will normally provide rules regarding the applicable safeguards.²⁹⁴ In Belgium, the same legal remedies apply to evidence obtained through indirect cooperation mechanisms (whether MLA or mutual recognition) as in the context of domestic procedures.²⁹⁵

From the perspective of admissibility, the legality of cross-border digital evidence gathered through indirect cooperation will be assessed in most countries according to the *locus regit actum* principle, which means that the procedural requirements of the requested or executing state must have been respected.²⁹⁶ In addition, the requesting or issuing state may also check if the evidence was collected in conformity with fundamental rights such as the right to privacy. For instance, Belgian courts will do this.²⁹⁷ The violation of a fundamental right will make the evidence unlawful, but this, however, does not automatically lead to its exclusion, as an *in concreto* assessment will have to be made (see Sections 16.4.2.2 and 16.4.3.5).²⁹⁸

²⁸⁶ Belgium, Chapter 9, 255–256.

²⁸⁷ SIRIUS EU Digital Evidence Situation Report, 62.

²⁸⁸ Ibid., 64.

²⁸⁹ Ireland, Chapter 12, 343–344.

²⁹⁰ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31–50.

²⁹¹ Ireland, Chapter 12, 344.

²⁹² Ibid., 310.

²⁹³ For example, Luxembourg, Chapter 13, 368–369.

²⁹⁴ Ibid., 368–369.

²⁹⁵ Belgium, Chapter 9, 256–257.

²⁹⁶ European Law Institute, ‘Explanatory Memorandum’, in *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings Draft Legislative Proposal of the European Law Institute* (Vienna: European Law Institute, 2023), 12. See also Bachmaier Winter and Salimi, *Admissibility of Evidence*.

²⁹⁷ Belgium, Chapter 9, 256.

²⁹⁸ Ibid., 256.

16.4.4.2 Cooperation of National Service Providers with Foreign LEAs

Cooperation of national service providers with foreign LEAs is based on the same instruments of transnational and international cooperation as apply in the reverse situation analysed in Section 16.4.4.1. As to voluntary direct cooperation, regulation is lacking as such, but in the EU context it meets strong limitations, contrary to the more permissive rules under US law.²⁹⁹ The GDPR constitutes a significant obstacle to voluntary transfer of data to foreign law enforcement and if there is no adequacy decision (Art. 45 GDPR) or appropriate safeguards (Art. 46 GDPR), only derogations under Article 49 GDPR could apply, and those are very limited.³⁰⁰ In that context it is worth recalling the Guidelines of the European Data Protection Board (EDPB), which clarified that ‘in situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to the existing MLAT or agreement’.³⁰¹ In the future, the EU obstacles to direct cooperation with US service providers could be lifted if the EU and the US are able to conclude a CLOUD Act Agreement.³⁰²

Voluntary cooperation of national service providers with foreign LEAs is not allowed in Estonia,³⁰³ Poland³⁰⁴ or Belgium.³⁰⁵ German law, too, is reluctant to permit its service providers to provide data voluntarily to foreign law enforcement authorities. Transfers of data to such authorities must be made with a valid legal basis, and unlawful disclosure violating secrecy of telecommunications may constitute a criminal offence. A breach of secrecy may be justified only in exceptional situations on grounds of necessity (§ 34 German Code of Criminal Procedure).³⁰⁶

It is, however, possible to find an exception to this general reluctance among the investigated legal systems. For instance, in Luxembourg, the expedited preservation measure available for domestic situations is also meant to apply if the request is issued by a foreign competent authority.³⁰⁷

16.5 CONCLUDING REMARKS: THE FUTURE IMPACT OF THE E-EVIDENCE REGULATION

From the analysis in this chapter, it is clear that direct cooperation presents a real challenge for cross-border gathering of digital evidence nowadays. Several authors report critical assessments of the MLA system, and even the EIO has been criticised as inadequate for gathering electronic evidence, for instance in Ireland³⁰⁸ and in Poland.³⁰⁹ In Luxembourg, too, these cross-border mechanisms are regarded as too slow. For instance, a source at the Luxembourg Ministry of Justice considered that it requires an average number of 120 days to receive electronic data requested from

²⁹⁹ See Chapter 21 (US), this volume.

³⁰⁰ See, e.g., EDPB, ‘Guidelines 2/2018 on Derogations of Article 49 under Regulation 2016/679’, adopted on 25 May 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf. See on this issue also Belgium, Chapter 9, 39/276.

³⁰¹ EDPB, ‘Guidelines 2/2018’, 5.

³⁰² See, e.g., P. Swire, ‘When Does GDPR Act as a Blocking Statute: The Relevance of a Lawful Basis for Transfer’, *Cross-Border Data Forum*, 4 November 2019, www.crossborderdataforum.org/when-does-gdpr-act-as-a-blocking-statute-the-relevance-of-a-lawful-basis-for-transfer/.

³⁰³ Estonia, Chapter 10, 286.

³⁰⁴ Poland, Chapter 14, 395.

³⁰⁵ Belgium, Chapter 9, 257.

³⁰⁶ Germany, Chapter 11, 306–307.

³⁰⁷ Luxembourg, Chapter 13, 364.

³⁰⁸ Ireland, Chapter 12, 338–339.

³⁰⁹ Poland, Chapter 14, 392–393.

an EU member state, and up to 300 days if the request is addressed to a third country (e.g. the US).³¹⁰ On the other hand, Estonian authorities are reportedly satisfied with the EIO.³¹¹

As a result, it is expected that the new system offered by the e-Evidence Regulation will have an important impact on cross-border gathering of electronic evidence as it will create a compelling unmediated way to obtain data from service providers while offering a protective legal framework, which is notably lacking at the moment.³¹² As was stated earlier, several countries tend to extend, unilaterally, their enforcement jurisdiction, thereby generating, however, potentially conflicting obligations for service providers called upon.³¹³

At the same time, it does not seem justified to expect the country where, by happenstance, the data is located to take responsibility for all users whose data is stored there. This problem is well illustrated by the *Skype* case. In this case, there was a conflict between the diametrically opposed approaches of Belgium and Luxembourg, provoking legal uncertainty for both service providers and the persons whose data was affected. According to the Luxembourg approach, it should be the guardian of all the data gathered by a service provider located within its territory, regardless of the nationality or residence of data subjects. In the Belgian approach, it should rather be the country where the service is offered (and thus the country of the affected users).³¹⁴

While the e-Evidence Regulation is meant to solve this conundrum,³¹⁵ putting this new system into practice will not be without hurdles. Implementing the Regulation into national legal orders will create a lot of questions.³¹⁶ For some member states, the e-Evidence Regulation may represent a less attractive alternative than what national law already offers (for instance, because national law does not require a judicial authorisation for the production of traffic data³¹⁷ or because it has a wider personal scope of application³¹⁸). Still, it will arguably not be possible to continue to use existing national rules in a cross-border context, as EU law prevails and the e-Evidence Regulation is meant to become the go-to instrument for direct cross-border cooperation. Whether this issue will generate litigation remains to be seen.³¹⁹

Furthermore, it is important to underline that the Regulation will not solve other important problems such as admissibility of evidence gathered through direct cooperation or encryption.³²⁰ The effectiveness of electronic evidence gathering will also be impacted by the rules and practice of data retention, which are fluctuating considerably in the absence of EU legislation.

More in general, our comparative research showed a lot of divergence in the rules applicable in the examined legal systems, starting with the definition of data and the types of service provider. While the e-Evidence Regulation brings welcome definitions of data categories, the EU framework unfortunately remains quite fragmented as far as the types of service provider are concerned. Across the seven EU member states, considerably variety exists with regard to cooperation with service providers. In some legal systems, voluntary cooperation is a key answer

³¹⁰ Luxembourg, Chapter 13, 368.

³¹¹ Estonia, Chapter 10, 284.

³¹² *Ibid.*, 286–287; Poland, Chapter 14, 397–398.

³¹³ For example, Germany, Chapter 11, 307–308.

³¹⁴ Luxembourg, Chapter 13, 370.

³¹⁵ Belgium, Chapter 9, 251–252.

³¹⁶ See, e.g., Luxembourg, Chapter 13, 372. See also S. Tosza, ‘The E-Evidence Package Is Adopted: End of a Saga or Beginning of a New One?’ (2023) 2 *European Data Protection Law Review* 163, 171–172; Franssen, ‘Cross-Border Gathering of Electronic Evidence in the EU’.

³¹⁷ Ireland, Chapter 12, 319.

³¹⁸ Belgium, Chapter 9, 257–259, in particular 258.

³¹⁹ See also Tosza, ‘The E-Evidence Package Is Adopted...’, at 172.

³²⁰ Franssen, ‘Cross-Border Gathering of Electronic Evidence in the EU’ at 208–209. See also Chapters 4 and 5, this volume. See also remarks in Ireland, Chapter 12, 344–346.

to avoid the cumbersomeness of the rules regarding international cooperation. Yet, at the same time, we also noted significant attempts to ‘domesticate’ transnational cases permitting the use of national rules.

For persons whose data is subject to transfer from service providers to LEAs, the legal remedies in the different legal systems diverge, too. A substantial limitation to the execution of the rights of those persons can be observed, for instance because of very strict time limits for questioning the applied measures or the lack of information. On the enforcement of service providers’ duties and penalties in the case of non-cooperation, striking discrepancies have emerged from the research, too.

Considering this national diversity, it is not surprising that the EU legislator has foreseen three years for the implementing process of the new e-Evidence Regulation. It will be of high relevance to observe how national rules will be shaped and how member states will supplement the rules of the Regulation where it leaves room for additional regulation (e.g. on remedies and sanctions).

Eventually this whole EU system will be placed in a broader international context as global service providers are also subject to rules in other countries, in particular the US, shaping their room for cooperation with EU law enforcement. This international context will be examined in Part III of the book, which will present the rules on gathering electronic evidence in five selected non-EU states – China, Russia, Turkey, the UK and the US – that are of crucial importance for contemporary internet governance.

PART III

Collecting Digital Evidence and the Role of Service Providers

A Global Perspective

Digital Evidence and Cooperation of Service Providers in China

Li Zhe and Jin Zhenan

17.1 INTRODUCTION

China has persistently insisted on respecting cyberspace sovereignty and data sovereignty.¹ In the National Cyberspace Security Strategy launched by the Cyberspace Administration Office, China explicitly declares that state sovereignty has expanded into cyberspace, and that cyberspace sovereignty has become an important part of state sovereignty.²

Service providers in China are under quite strict control. They are obliged to retain certain data and to cooperate with authorities in both administrative proceedings and criminal investigations, as required by criminal and administrative laws, as well as more than thirty administrative regulations targeting different types of service providers. Due to the comprehensive and multifaceted administrative regulations on service providers and the mandatory requirement to store certain data within the territory of China, the cooperation of service providers in the process of both administrative proceedings and criminal investigations is quite successful domestically. There is no strong demand from the Chinese government for data retention by service providers; only a limited number of service providers are required to retain traffic data, normally for a period of sixty days.³

As to evidence collection in criminal proceedings, the Chinese Criminal Procedure Law (CPL)⁴ does not satisfactorily differentiate collection of electronic evidence from collection of other physical evidence, nor does it distinguish the cooperation obligations of service providers from those imposed on other persons or entities, since there is only a general provision requiring that all the concerned personnel or entities shall provide evidence when ordered to do so by the investigative authority. As will be explained in this chapter, these provisions are supplemented by interpretations, guidelines and provisions adopted by different authorities; these supplementary documents function as ‘loophole fillers’ in some way, to meet the needs of specific investigative situations. But this approach results in some conflicts between the various applicable

¹ See, e.g., Yu Zhigang, ‘The Concept of Cyberspace Sovereignty and the Innovation of Theories on the Rule of Law’, *Guangming Daily*, 11 September 2016, 1, http://epaper.gmw.cn/gmrb/html/2016-09/11/nw.D110000gmrb_20160911_7-01.htm?div=1 (in Chinese).

² Cyberspace Administration of China, The National Cyberspace Security Strategy, 27 December 2016, www.cac.gov.cn/2016-12/27/c_1120195926.htm (in Chinese).

³ For example, Interim Provisions on the Administration of Internet Culture (IPAIC), 15 December 2017, Art. 20, http://zwgk.mct.gov.cn/zfxgkml/zcfg/bmgz/202012/t20201204_905340.html (in Chinese); Provisions on the Administration of Internet Live-Streaming Services (Provisions AILSS), 4 November 2016, Art. 16, www.cac.gov.cn/2016-11/04/c_1119847629.htm (in Chinese).

⁴ Adopted in 1979 and amended in 1996, 2012 and 2018. The following discussion is based on the 2018 version unless specified otherwise Chinese Criminal Procedure Law (CPL), 26 October 2018, www.npc.gov.cn/zgrdw/npc/xinwen/2018-11/05/content_2065631.htm (in Chinese).

documents – conflicts that need to be resolved. Without being rooted in the CPL, the newly created investigative methods⁵ described by such documents actually lack justification. This chapter will examine this multilayered legal framework for electronic evidence collection, as well as the cooperation obligations thereof, followed by several comments to improve current Chinese practice.

Furthermore, in response to the rapid progress in data-dominated society, China has promulgated several laws, including the Cybersecurity Law,⁶ the Data Security Law⁷ and the Personal Information Protection Law (PIP Law),⁸ to form a new order of data governance. However, with regard to cross-border cooperation in collection of electronic evidence, according to the Law on International Criminal Judicial Assistance (ICJA Law),⁹ traditional mutual legal assistance is still the main approach, or even the only feasible approach.¹⁰

Partly serving as a response to the American Clarifying Lawful Overseas Use of Data Act (CLOUD Act),¹¹ China has strengthened data localisation as a criterion to claim jurisdiction,¹² and requires that certain operators or service providers store certain types of data domestically. This includes information domestically generated or collected by critical information infrastructure operators, and the data domestically generated or collected by personal information processors that deal with a huge quantity of personal information.¹³ Meanwhile, institutions, agencies and individuals within the territory of China are forbidden from providing evidentiary material and assistance prescribed by this Law to foreign countries without the approval of the competent authority of China.¹⁴ Although the mandatory data localisation policy reduces the difficulty of collecting electronic evidence for Chinese law enforcement authorities (LEAs), the issue of cross-border cooperation in collecting electronic evidence is still an unavoidable question.

17.2 SETTING THE SCENE

17.2.1 *General Approach to the Collection of Electronic Evidence*

The laws adopted by the legislature, the National People's Congress and its Standing Committee, are usually abstract, which leaves space for interpretations, administrative regulations, guidelines and rules. There are two main types of interpretations: legislative interpretations by the Standing Committee of the National People's Congress; and judicial

⁵ These methods include on-site extraction of electronic data, online extraction of electronic data and freezing electronic data.

⁶ Cybersecurity Law, 7 November 2016, www.npc.gov.cn/zgrdw/npc/zfjc/zfjcelys/2016-11/07/content_2034939.htm (in Chinese).

⁷ Data Security Law, 10 June 2021, www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml (in Chinese).

⁸ Personal Information Protection Law (PIP Law), 20 August 2021, www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (in Chinese).

⁹ Law on International Criminal Judicial Assistance (ICJA Law), 26 October 2018, www.npc.gov.cn/zgrdw/npc/xinwen/2018-10/26/content_2064576.htm (in Chinese).

¹⁰ ICJA Law, Art. 4; PIP Law, Art. 41; Data Security Law, Art. 36.

¹¹ Clarifying Lawful Overseas Use of Data Act (CLOUD Act) of March 2018, www.justice.gov/criminal-oia/page/file/1152896/download.

¹² ICJA Law, Art. 25.

¹³ Cybersecurity Law, Art. 37; PIP Law, Art. 40; Data Security Law, Art. 31.

¹⁴ ICJA Law, Art. 4; PIP Law, Art. 41; Data Security Law, Art. 36.

interpretations by the Supreme People's Court and the Supreme People's Procuratorate.¹⁵ Contrary to an interpretation of law in a specific case or cases, the judicial interpretations of law by the prosecution offices and courts in China supplement the laws and are issued as guidance in a general manner.¹⁶ Administrative regulations, guidelines and rules are enacted by the central government (the State Council), local governments and the ministries of the State Council.

The collection of electronic evidence is regulated very generally in the CPL, while most of the provisions concerning the collection of electronic evidence can be found in legislative interpretations, judicial interpretations, administrative regulations, guidelines and rules. This complex legal framework will now be analysed in more detail.

According to the 1996 CPL, the only type of evidence in electronic form was audiovisual material. In 2012, electronic data was added to the CPL as another type. However, the collection, identification and appraisal of electronic evidence was still not concretely regulated in the CPL.

In 2016, in order to meet the needs of judicial practice, the Supreme People's Court, the Supreme People's Procuratorate and the Ministry of Public Security jointly issued the Provisions on Several Issues Concerning the Collection, Taking, Examination and Judgment of Electronic Data in the Handling of Criminal Cases (Joint Provisions).¹⁷ In 2019, based on the Joint Provisions, the Ministry of Public Security issued Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases (Rules MPS)¹⁸ to further elaborate and clarify the Joint Provisions. The Rules MPS and the Joint Provisions have become the main resources for regulating collection of electronic evidence in Chinese criminal procedure, including the cooperation of service providers. The detailed provisions on this cooperation will be analysed in Section 17.4.2. Moreover, the Provisions on the Procedures for Handling Criminal Cases by Public Security Agencies (Provisions PSA),¹⁹ previously published by the Ministry of Public Security in 2012, were amended in 2020, adding some collection methods of electronic evidence provided in the Rules MPS.

To ensure their cooperation in criminal and administrative proceedings, service providers are required to retain data, preserve and disclose electronic data, as well as protect data privacy, respect data localisation and meet obligations with regard to cross-border transfer. Such obligations can be found in recently promulgated laws, namely the Counterterrorism Law,²⁰ the Cybersecurity Law, the Data Security Law and the ICJA Law. There are also more than thirty administrative regulations that specify these obligations of service providers.²¹ To summarise,

¹⁵ The People's Procuratorate is the official English name of what is called the public prosecutor's office in other legal systems. The following discussion will use the terms prosecution office and prosecutor, except when referring to the Supreme People's Procuratorate.

¹⁶ Chen Chunlong, 'On the Status and Functions of Chinese Legal Interpretations' (2013) 1 *China Legal Science* 24–25 (in Chinese).

¹⁷ Supreme People's Court, Supreme People's Procuratorate and Ministry of Public Security, 'The Provisions on Several Issues Concerning the Collection, Taking, Examination and Judgment of Electronic Data in the Handling of Criminal Cases' (Joint Provisions), 9 September 2016, www.spp.gov.cn/xwfbh/wsfbt/201609/t20160920_167380_1.shtml (in Chinese).

¹⁸ Ministry of Public Security, 'Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases' (Rules MPS), 2 January 2019, <https://app.mps.gov.cn/gdnps/pc/content.jsp?id=7449892> (in Chinese).

¹⁹ Provisions on the Procedures for Handling Criminal Cases by Public Security Agencies (Provisions PSA), 20 July 2020, www.gov.cn/zhengce/2021-12/25/content_5712867.htm (in Chinese).

²⁰ Counterterrorism Law, 27 April 2018, www.npc.gov.cn/zgrdw/npc/xinwen/2018-06/12/content_2055871.htm (in Chinese).

²¹ Among these regulations, some are general, namely the Decision of the Standing Committee of the National People's Congress on Strengthening Online Information Protection and the Provisions on Protecting the Personal

rules on data retention and the cooperation of service providers in criminal investigations in China can be found in criminal laws, supplementary legal documents, administrative laws and administrative regulations, as will be discussed in Sections 17.2.2 and 17.4.3.

17.2.2 Data Retention Obligations

17.2.2.1 Introduction

The PIP Law safeguards the security and privacy of users' information by setting up basic principles for the processing of personal information. Personal information refers to all kinds of information related to identified or identifiable natural persons that are electronically or otherwise recorded, excluding information that has been anonymised. Personal information processing includes the collection, storage, use, processing, transmission, provision, disclosure and deletion of personal information (Article 4 of the PIP Law). Information processing must follow the principle of lawfulness, legitimacy, necessity and good faith (Article 5) as well as the principle of openness and transparency (Article 7). Also, the following conditions must be fulfilled: obtaining the consent of users (Article 13); limiting the processing to that directly related to the processing purpose and in a manner that has the minimum impact on the rights and interests of individuals; and limiting the collection to the minimum scope necessary for achieving the processing purpose (Article 6).

Besides the collection and preservation of users' personal data for their own business purposes, service providers are under certain data retention obligations. However, the scope of data retained in China has a wider scope than personal information. Service providers are mostly required to retain users' traffic data, but certain types of service providers must also keep content data. That said, the content data to be retained is not the content of users' private communication but rather that of the products published by service providers or users. For example, online publishing service providers must retain the content of digital works they published online;²² internet live-streaming service providers must retain the content that their users published.²³

In most data retention cases, data is required to be retained in the servers of the service provider for a certain period (see Section 17.2.2.2), but in certain special circumstances, data must be handed over for record-filing to the Cyberspace Administration Office of China (in Chinese: Bei An) (see Section 17.2.2.3).

17.2.2.2 Data Retention in the Data Servers of Service Providers

The period for data retention varies according to the different types of service providers, as regulated in different administrative regulations. Service providers must preserve the data for a certain period of time, usually sixty days. For example, Article 20 of the Interim Provisions on

Information of Telecommunications and Internet Users, while others regulate only certain types of service provider, such as internet culture service providers (IPAIC), online publishing service providers (Provisions on the Administration of Online Publishing Services (Provisions AOPS), 4 February 2016, Art. 34, www.nppa.gov.cn/nppa/contents/770/103241.shtml (in Chinese)) and information service providers (Administrative Measures for Internet Information Services). Information service provider is a typical type that includes mobile internet applications information service providers (Provisions AMIAIS), news information service providers (Provisions for the Administration of Internet News Information Services (Provisions AINIS), CLI4.293919, 2 May 2017, www.cac.gov.cn/2017-05/02/c_1120902760.htm) and so on.

²² Provisions AOPS, Art. 34.

²³ Provisions AILSS, Art. 16.

the Administration of Internet Culture²⁴ states that internet cultural entities must retain the times of dissemination, the uniform resource locators (URLs) or domain names and the content of internet cultural products they provide for sixty days; Article 16 of the Provisions on the Administration of Internet Live-Streaming Services requires that internet live-streaming service providers retain logs of internet live-streaming service users and the content that they published for sixty days.

Sometimes the preservation period will be longer, depending on the applicable legislation. For example, the Interim Measures for the Administration of the Business Activities of Online Lending Information Intermediary Institutions²⁵ provide that network-based lending information intermediary agencies must record the internet access log, particulars of information interaction and other data of both lenders and borrowers and keep such data for five years from the expiry of the loan contract (Article 18, paragraph 2).

17.2.2.3 Record-Filing of Information to the Cybersecurity Administration Office of China

Ordinarily, data retention is conducted as storing the retained data on the service providers' own data servers. Nevertheless, certain types of service providers must preserve the data in another way: by putting it on record with the corresponding national or local Cyberspace Administration Office.

This record-filing method is a stricter approach to ensure cybersecurity, only targeting microblog service providers, public account information service platforms, internet news information services and public information services provided through instant messaging tools. The rationale for this more stringent requirement is that public accounts must fulfil their social responsibilities, avoiding the publishing of illegal information on mass or social media.

Article 9 of the Provisions on the Administration of Microblog Information Services,²⁶ Article 14 of the Provisions for the Administration of Internet News Information Services²⁷ and Article 7 of the Interim Provisions on the Administration of the Development of Public Information Services Provided through Instant Messaging Tools²⁸ contain similar requirements about this record-filing obligation. Providers of such information services must put users' accounts, service qualification of users' public accounts (to permit or license posting certain kinds of information, such as public news) and certain other information on record.

²⁴ IPAIC, Art. 20.

²⁵ Interim Measures for the Administration of the Business Activities of Online Lending Information Intermediary Institutions (IM for BAOLI), 17 August 2016, https://wap.miit.gov.cn/zcfg/xxxtl/art/2016/art_704cdd6af63c4071ba f9ac837c5b08fd.html (in Chinese). The term 'online lending information intermediary institution' refers to financial information intermediary institutions legally formed to specially conduct online lending information intermediary business activities. Such type of institutions take the internet as the primary channel and provide information search, information release, credit rating, information exchange, credit matching and other services for direct lending between borrowers and lenders (IM for BAOLI, Art. 2).

²⁶ Provisions on the Administration of Microblog Information Services (Provisions AMIS), 2 February 2018, www.cac.gov.cn/2018-02/02/c_1122358726.htm (in Chinese).

²⁷ Provisions AINIS, Art. 14.

²⁸ Interim Provisions on the Administration of the Development of Public Information Services Provided through Instant Messaging Tools, 7 August 2014, Art. 7, https://www.cac.gov.cn/2014-08/07/c_1111983456.htm (in Chinese).

17.3 TERMINOLOGY AND CATEGORISATIONS

17.3.1 Data

17.3.1.1 Terminology

The Joint Provisions define the term ‘electronic data’ in Article 1: ‘Electronic data is stored, processed and transmitted in electronic form and can be used to prove the facts of the case.’²⁹ In judicial practice, electronic data and electronic evidence are the two commonly used terms, with no significant difference between them.

17.3.1.2 Categorisations

Article 1 of the Joint Provisions also includes a non-exclusive list of forms of electronic data:

Electronic data includes but is not limited to the following information and electronic documents:

- (1) Information published through such network platforms as webpage, blog, microblogs,³⁰ moments,³¹ post bar,³² and network drive.
- (2) Communication data in such network application services as SMS, e-mail, instant messaging, and group chat.
- (3) Information including user subscriber information, identity authentication information, electronic trading records, communication records, and log-on logs.
- (4) Electronic documents including documents, pictures, audio and video records, digital certificates, and computer programs.

The first type of electronic data published on internet platforms can be seen as public information, the collection of which does not entail infringement of individual rights and can thus take place with fewer limitations. The other three types of electronic data are more related to communication information of individuals, privacy and business secrets, the obtainment of which is more likely to cause conflict with individual rights³³ and requires a more stringent approval procedure. However, whether ‘moments’ postings on Wechat (a very popular communication app) are private or public information is still under discussion.³⁴ Moments are supposed to be open to all the contacts of the Wechat account owner who posted the moments, but if you are not listed in the contacts of the Wechat account owner, then either you cannot get access to the moments or you can get only limited access to them, depending on the settings of the Wechat account owner.

²⁹ All provisions quoted in this chapter have been translated into English by the authors.

³⁰ A microblog is a similar format to X (formerly Twitter) that is popular in China; it allows users to instantly update short texts and publish them publicly.

³¹ Here, ‘moments’ refers in particular to a function of Wechat. Wechat is an instant messaging tool developed by Tencent Co Ltd. On the Moments page, users can publish photos and text (referred to as ‘moments’) and choose who can view them and comment on them.

³² Post bar, or *Tieba* in Chinese, is a bulletin board system website where people sharing the same interests discuss and interact under their interested topics. Currently, the largest Chinese post bar is *Baidu Tieba* hosted by Chinese search engine company *Baidu*.

³³ Long Zongzhi, ‘Seeking for the Balance of Effective Evidence Collection and the Guarantee of Rights: A Comment on Provisions in the Joint Provisions about Electronic Evidence’ (2016) 11 *Law Science* 8 (in Chinese).

³⁴ See Pan Xiaoshuang and Yue Yuanzheng, ‘Analysis on the Tendency of Compromising Private and Public Space of Wechat Moments’ (2016) 4 *Radio & TV Journal* 147–148 (in Chinese).

17.3.2 Service Provider

The term ‘service provider’ appears in several laws and regulations. The first definition of ‘service provider’ in criminal law can be found in 2019 in a supplementary document jointly issued by the Supreme People’s Court and the Supreme People’s Procuratorate, entitled *Interpretations on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving Crimes of Illegally Using an Information Network or Providing Aid for Criminal Activities in Relation to Information Network* (Interpretations IN).³⁵ That said, the term ‘service provider’ has been used in legislation long before it was defined in legal documents.

The Regulation on Telecommunications (RT)³⁶ first gives a list of all the types of telecommunication services³⁷ provided in China, as well as the corresponding licences that are needed before operating telecommunication services. The term ‘telecommunication’ here refers to ‘the use of wired or wireless electromagnetic systems, or photoelectric systems, to transmit, emit or receive speech, text, data, graphics or any other form of information’ (Article 2 of the RT). Telecommunication service providers are divided into basic telecommunication business providers and value-added telecommunication business providers (Article 8 of the RT). Basic telecommunication business refers to the provision of infrastructure of public networks, public data transmission and basic speech communication. So the providers of basic telecommunication business are the so-called carriers or telecommunication operators. Value-added telecommunication business refers to the provision of telecommunication and information services by using the infrastructure of public networks. There are eleven types of value-added telecommunication businesses. Among the eleven types, operators of internet access services (Type B14) must apply for an ISP (internet service provider) licence, whereas operators of internet information services (Type B25) must apply for either an ICP (internet content provider) licence, if the service is provided via the internet, or an SP (service provider) licence, if the service is provided via a non-internet network such as a fixed telecommunication network or a mobile communication network. However, the term ‘service provider’ in criminal procedure does not merely refer to providers with ISP, SP or ICP licences; it embraces all eleven types and even new types of telecommunication business that have not yet been regulated in the list.³⁸

The Cybersecurity Law uses the term ‘cyberspace operators’, which refers to the owners and managers of cyberspaces, and cyberspace service providers (paragraph 3 of Article 76). However, the law does not further define the terms ‘cyberspace owner’, ‘manager’ and ‘service provider’. Next, Article 24 of the Cybersecurity Law states that the service involved includes cyberspace access services, domain name registration services, access formalities for fixed-line telephone or mobile phone, information release and instant messaging. Articles 18 and 19 of the Counterterrorism Law³⁹ mention the terms ‘telecommunication operators’ and ‘internet service

³⁵ Supreme People’s Court and Supreme People’s Procuratorate, ‘Interpretations on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving Crimes of Illegally Using an Information Network or Providing Aid for Criminal Activities in Relation to Information Network’ (Interpretations IN), 21 October 2019, www.cac.gov.cn/2019-10/25/c_1573534999086260.htm?from=singlemessage (in Chinese).

³⁶ Regulation on Telecommunications (RT), 6 February 2016, www.gov.cn/zhengce/2020-12/26/content_5574368.htm (in Chinese).

³⁷ The list in force was issued in 2015 and amended in 2019.

³⁸ Based on Article 9 of the RT, telecommunication operators can operate new-type telecommunication business not covered by the list after they record the business at the telecommunication administrative authority.

³⁹ Counterterrorism Law, 27 April 2018, www.npc.gov.cn/npc/c30834/201806/d256505a5c254abdb07e2ff5d892d5d6.shtml (in Chinese) is administrative law in nature, regulating the system through which the government prevents and responds to terrorist activities. The crimes with regard to terrorism are provided in Articles 120 and 120-1 to 120-6 of the Criminal Law, 26 December 2020, www.npc.gov.cn/wxzlhg/b2021/202104/3a338df89b0a415481a9b0f571588f88/files/3d9248e01141484ead7d01b58958e0ae.pdf (in Chinese).

providers' when talking about the cooperation of service providers with the government and the police to fight against terrorism.

Furthermore, moving to the sphere of criminal law, Article 286-1 of the Criminal Law,⁴⁰ as amended in 2015, first used the term 'service providers' when it incriminated the action of 'refusing to perform the information network security management obligation'.⁴¹ A service provider may commit the crime of failure to perform the information network security management obligation if it fails to fulfil its network security management obligation and refuses to correct its acts upon the competent authorities' order, thereby causing serious consequences.

The first definition of the term 'service provider' in the criminal law field appears in 2019 in the Interpretations IN. The Interpretations IN specify in Article 1 the elements of the aforementioned crime, 'refusing to perform the information network security management obligation', including a definition of service provider.

In accordance with Article 1 of the Interpretations IN, agencies, companies and individuals providing the following services shall be considered 'network service providers' as provided in paragraph 1 of Article 286-1 of the Criminal Law:

- (1) Network access, DNS (or Domain Name Server) resolution, and other information network access, computing, storage, or transmission services;
- (2) Information releasing, search engines, instant messaging, online payment, online booking, online sales, online games, online live-streaming, website construction, security protection, advertisement promotions, app stores, and other information network application services;
- (3) public services such as e-governance, communications, power, transportation, water, finance, education, and medical care provided via information networks.

However, the service providers defined under the cooperation obligation provided in the CPL may cover a far more extensive range: all the 'relevant entities or individuals' as provided in Article 54 of the CPL are indiscriminately under the obligation to cooperate with the police in the framework of a criminal investigation. This includes, for instance, the suspect's school, employer or bank which may store individuals' data, but the relevant entity may also include any type of telecommunication operator and network service provider. Therefore, it can be concluded that in China, all telecommunication-related and internet-related entities are under a general obligation to cooperation with the prosecution office and the public security agency⁴² in criminal investigations, although the details of cooperation agencies may slightly vary depending on the type of organisation.

17.4 DOMESTIC COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

17.4.1 *Introduction*

As explained in Section 17.3.2, the CPL entails a general cooperation obligation for service providers, as well as other relevant entities and individuals, to provide evidence and assistance during criminal investigations. In accordance with Article 52 of the CPL, judges, public prosecutors and investigators must ensure that all citizens who are involved in a case or who

⁴⁰ Criminal Law, Art. 286-1.

⁴¹ For the definition of information network security management obligation, see Section 17.4.4.2.

⁴² Usually, it is the public security organisations that investigate criminal cases, but the prosecution offices, the state security organisations and the prisons are responsible for investigation of certain crimes as provided by law.

have information about the case provide all available evidence and, except under special circumstances,⁴³ may ask such citizens to provide assistance in the investigation.

In China, the term LEAs covers all the authorities that enjoy investigative powers in criminal cases. The public security organisation is not the only authority investigating criminal cases; the national security authority,⁴⁴ the armed forces, the China Coast Guard, the prison,⁴⁵ the oversight commission (i.e. the anti-corruption agencies in China)⁴⁶ and the prosecution office⁴⁷ also enjoy certain investigative powers in specific cases. The provisions in the CPL generally describe the collection of electronic evidence powers of all the investigative agencies, except the investigative power of the oversight commissions, which is regulated in the Oversight Law. The concrete methods applicable to each authority are described in their corresponding supplementary documents, which results in slightly different investigative methods for each authority. For convenience, the following discussion will focus on the police and their powers, representing LEAs more in general.

Article 54 of the CPL states that when the courts, the prosecution offices or the public security agencies⁴⁸ collect and obtain evidence from the relevant entity or individual, the latter shall truthfully provide the requested evidence. The Counterterrorism Law, the Cybersecurity Law and the Data Security Law contain a specific cooperation obligation for service providers. In accordance with Article 18 of the Counterterrorism Law, both telecommunications business operators and internet service providers must provide technical interface, decryption and other technical support and assistance to the public security authorities and the national security authorities for the prevention and investigation of terrorist activities. Article 28 of the Cybersecurity Law states that service providers must provide technical support and assistance to public security agencies and national security agencies that are safeguarding national security and investigating criminal activities as required by law. Additionally, in accordance with Article 35 of the Data Security Law, service providers must cooperate with public security authorities or national security authorities for the purpose of maintaining national security or investigating crimes.

Moreover, according to Article 54 of the CPL, the evidence obtained during administrative proceedings can also be used as evidence in a criminal case. This shows that there is a close connection between criminal and administrative proceedings.

⁴³ For example, a physically or mentally handicapped person or a minor who cannot distinguish between right and wrong or cannot correctly express themselves will not serve as a witness (CPL, Art. 62). The spouse, a parent or a child of the defendant has the right to refuse to testify before court as a witness (CPL, Art. 193).

⁴⁴ Article 4 of the CPL provides that when handling criminal cases regarding compromising national security, the national security authorities perform the same functions as those of public security authorities.

⁴⁵ The security department of the armed forces has the authority to investigate criminal cases that occur within the armed forces; the China Coast Guard exercises the authority to investigate criminal cases that occur at sea; the prison investigates crimes committed by convicts within the prison (CPL, Art. 308).

⁴⁶ The oversight commission is responsible for investigating duty-related violations and crimes committed by public officials that exercise public power, such as suspected corruption, bribery, abuse of power, neglect of duty, power rent-seeking, tunnelling, practice of favouritism and falsification, as well as the waste of state assets (Oversight Law, 20 March 2018, Arts. 3, 11, www.npc.gov.cn/npc/c30834/201803/c69c51c278f24ebab91b2178a4498404.shtml).

⁴⁷ The prosecution office is competent to investigate crimes committed by any justice functionary of false imprisonment, extortion of a confession by torture, or illegal search or any other crime that infringes upon a citizen's rights or damages the fair administration of justice by taking advantage of his or her functions. Where a case regarding a serious crime committed by any staff member of a government authority by taking advantage of his or her functions under the jurisdiction of a public security authority needs to be directly accepted by a prosecutor, the prosecutor may also have investigative power (CPL, Art. 19).

⁴⁸ In China, 'public security organisations' refers to a type of police that is responsible for maintaining public order and for preventing and investigating crimes. The police in China consist of police in public security organisations, state security organisations, prisons and organisations in charge of re-education through labour, as well as judicial police in courts and prosecution offices.

Therefore, in this section, we will discuss two questions. Firstly, we will present the detailed criminal procedures of how service providers cooperate with the police as stipulated in the CPL and the complementary regulations, guidelines and rules (see Section 17.4.2). Secondly, we will analyse how criminal investigations are connected to and influenced by the daily process of administrative supervision and control (see Section 17.4.3).

17.4.2 Cooperation in Criminal Investigations

In judicial practice, there are many cases where service providers cooperate with investigators in criminal investigations. Case-law research was conducted in Zhejiang Province (where China's biggest e-commerce company, Alibaba, is situated). The research was conducted on a sample of 483 cases from 1996 to 2016 in which the use of electronic evidence was explicitly mentioned. The results show that 109 out of the 483 cases include electronic evidence provided by a third party.⁴⁹

Some cooperation practices have developed into conventional mechanisms, although they are not regulated in any specific legal documents. For example, in 2015, the State Council approved the establishment of the Inter-ministerial Joint Meeting on Matters Concerning the Work of Combating and Controlling New Telecommunication Network-Related Illegal and Criminal Activities. The government entities involved are the Ministry of Public Security and twenty-two other ministries. This joint meeting is a long-term multi-sector cooperation mechanism to fight against crimes of fraud through telecommunication networks. In the framework of this joint meeting, each province has established an anti-fraud centre that includes representatives of the three basic telecommunication companies – China Mobile, China Unicom and China Telecom – to facilitate the operations of the centre. This centre quickly disconnects phone numbers allegedly involved in telemarketing scams and shares relevant information with service providers and the police to suspend payments immediately.⁵⁰ This cooperation mechanism has already proven to be effective in 1,550,000 telecommunication fraud cases and, in the first nine months of 2020, a direct loss of 100 billion CNY was retrieved.

In Section 17.4.2.1, we will discuss the legislation of electronic data collection methods. This includes historical data and real-time data, and how service providers are required to cooperate in each of the methods.

17.4.2.1 Cooperation Obligations of Service Providers in the Collection of Historical Electronic Data

Service providers' participation and cooperation play an important role in gathering or extracting electronic data. Such participation and cooperation are basically regulated in the Provisions PSA, the Joint Provisions and the Rules MPS,⁵¹ including obligations to provide assistance, to

⁴⁹ See, e.g., Feng Jiao, 'The Collection of Internet Evidence' (2018) 26 *Journal of National Prosecutors College* 36 (in Chinese). The author studied the criminal cases included in the judicial database PKULAW that happened in Zhejiang Province from 1996 to 2016 and were related with electronic data. The author identified 1,020 cases in total and 483 after excluding those that were substantively irrelevant.

⁵⁰ Zhang Yang and Wei Zhezhe, 'Focus on Fights against Telemarketing Scams: Inter-ministerial Joint Meeting of 23 Ministries', *People's Daily*, 14 September 2016, 2 (in Chinese).

⁵¹ The Rules MPS have been developed from the Joint Provisions. The methods of electronic evidence collection provided in these two regulations are the same, but the Rules MPS adjust some details of the provisions. In the discussion that follows, we will therefore focus more on the Rules MPS.

preserve the original storage media, to produce electronic evidence at the request of the police and to freeze electronic data.

17.4.2.1.1 PROVIDING ASSISTANCE TO THE POLICE FOR COLLECTING ELECTRONIC DATA. Service providers may need to provide assistance when the police seize the original storage medium or extract electronic data on site⁵² or online. In view of this seizure, the police must follow certain procedures as regulated in the Provisions PSA and the Rules MPS.

To seize original storage media, the police must deliver a written seizure order approved by the director of the case-handling department. Where it becomes necessary to seize property or assets on site during an inspection or a search, the person in charge at the scene has to make the decision. Where the property is highly valuable or its seizure might seriously impact routine business, the seizure must be done with a written Seizure Decision approved by the principal of the public security organisation at the county level or above (Article 228 of the Provisions PSA).

To extract electronic data on site, a record of on-site extraction of electronic data must be made. The investigators and the person in possession of, or providing, the electronic data are to sign it or affix a seal; if the aforementioned person is unable to sign or refuses to do so, this shall be noted in the record and an authenticating witness is to sign or affix a seal (Article 19 of the Rules MPS).

To extract electronic data online, the source, subject, goals and targets of the online extraction of electronic data must be indicated in the record, as well as the time, place, method and process of the extraction, and the reasons for being unable to seize the original storage media. An inventory of extracted and fixed electronic data is to be attached, indicating the type, document format, integrity check value and so on, and the investigators need to sign it or affix a seal (Article 26 of the Rules MPS).

For online remote inspections, the county-level public security agencies handling the case are the responsible authority (Article 28 of the Rules MPS) and the inspection process must be witnessed by qualified personnel (Article 30 of the Rules MPS). After remote inspections are concluded, a Remote Inspection Record must be promptly made, recording in detail the relevant circumstances as well as the inspection content such as pictures or screenshots; the investigators and the authenticating witnesses are to sign it or affix a seal (Article 31 of the Rules MPS).

The assistance given by service providers in this process can be threefold. First, when the police come to seize the original storage media or extract electronic data on site, service providers must not interfere with the police's work.

Second, when the investigators seize the original storage media, service providers must provide relevant information on request as far as they know, such as information about the original storage media and application systems, network topology and system layout, the identity of the users or managers, the user names and passwords for the original storage media and application systems, and the circumstances of data backups for the original storage media, that is, whether there are encrypted disks or containers, whether there are other mobile media, whether backups have been made, the location of backup storage data and so on (Article 15 of the Rules MPS).

Third, when making online extractions or remote online inspections, investigators must use the remote computer information access system (Article 33 of the Rules MPS), such as user names and passwords provided by the person in possession of the electronic data or network

⁵² 'On site' means that the LEAs have the relevant computers or servers at hand.

service providers. This means that without their cooperation, the online extractions and remote online inspections could not succeed.

17.4.2.1.2 PRESERVING THE ORIGINAL STORAGE MEDIA. Service providers may need to preserve the original storage media when the original storage media cannot be seized and the electronic data cannot be extracted at once. In accordance with paragraph 2 of Article 22 of the Rules MPS, service providers must appropriately keep the original storage media and must not transfer, sell or destroy it; they must not unseal it; they must not access networks without the permission of the case-handling departments; and they must not add to, delete or modify electronic data which might be used as evidence. When necessary, the computer information system must be left in a turned-on state.

The procedure to give the original storage media to the service provider for preserving is also regulated in paragraphs 1 and 3 of the same article: The original storage media must be sealed after registering, photographing or video recording. Two copies of a registered preservation list must be made and signed or have a seal affixed by the investigators, the persons in possession (providers) and the authenticating witnesses. One copy of the list must be given to the persons in possession of the original storage media (providers) and the other copy must be put in the file along with the pictures or video. The police must decide on the disposition of the original storage media within seven days; where the decision is not made within this period, the order will be considered automatically lifted. Where they are confirmed as being unrelated to the case under investigation, the devices must be released within three days.

17.4.2.1.3 PRODUCING ELECTRONIC DATA. Service providers must produce data as required by the police. The difference between the obligation of providing assistance and that of producing electronic data lies in that when service providers provide assistance, it is the police that collect the evidence, but when producing electronic data, the electronic data is directly collected by the service providers.

To request service providers to produce data related to a criminal case, in accordance with Article 41 of the Rules MPS, the police must get approval from the director of the case-handling department and issue a notice of evidence collection to the service providers. The notice of evidence collection must specify relevant information about the electronic data targeted. The service providers must sign or seal the notice of evidence collection; if they refuse to sign or seal it, the police must note this. When necessary, methods such as audio or video recording can be used to fix the content of the evidence and the process of evidence gathering. Article 62 of the Provisions PSA states that the notice of evidence collection must clearly specify the evidence to be collected and the time limit for collection.

The Provisions PSA also regulate the procedure for the public security agencies to request service providers to provide emails. The seizure of suspects' email, as well as their mail and telegrams, must be approved by the principal of the public security organisation at or above the county level with a seizure order, requiring the post and telecommunications offices or service providers to check and hand over the relevant mail, telegrams or email for seizure. When there is no longer any need for seizure, the service providers must be notified to end the process (Article 232 of the Provisions PSA). If, upon verification, the email is found to be not relevant to the case, the seizure must be ended within three days (Article 233 of the Provisions PSA).

17.4.2.1.4 FREEZING ELECTRONIC DATA. Freezing will be employed in the following conditions: when there is a large volume of data that cannot be collected, or it is inconvenient to do so;

when the extraction time is long and might cause the electronic data to be tampered with or destroyed; or when the electronic data can be more intuitively displayed through network applications (Article 36 of the Rules MPS).

Service providers must freeze and unfreeze electronic data as ordered by the police. One or more of the following methods must be employed when freezing electronic data: calculating the electronic data's integrity check value; locking network application accounts; employing write-protection measures and other measures to prevent the addition, deletion or modification of electronic data (Article 40 of the Rules MPS).

The police must issue a notification of assistance in freezing electronic data or a notification of unfreezing of electronic data approved by the principal of a public security organisation at the county level or above, to the person in possession of the electronic data, the network service providers or relevant departments. The notification of assistance in freezing electronic data must state information such as the web accounts of the targeted data (Articles 37 and 38 of the Rules MPS).

The period for freezing electronic data is six months. Where it is necessary to extend the time limits due to special circumstances, the public security organisation must complete the procedures for continuation of the freezing before expiry of the freezing period. The period for each extension of freezing must not exceed six months. Where freezing is continued, the freezing procedure must be renewed. Where the period is exceeded without handling procedures, it is viewed as automatic unfreezing (Article 39 of the Rules MPS).

17.4.2.2 Collection of Real-Time Data as a Technical Measure

Paragraph 2 of Article 33 of the Rules MPS encompasses technical measures for collecting data in real time: when using technical measures to collect electronic data, approval procedures must be instituted in strict accordance with the relevant rules. The rules are provided in Part 2, Chapter 2, Section 8 of the CPL.

Technical investigative measures are used in criminal cases to secretly collect evidence related to suspects or persons with direct links to criminal activities, including monitoring records, tracing movements, intercepting communication and surveilling places. The scope of records monitored includes call records, consumption records of credit cards or debit cards, hotel check-in records and internet logs; tracing movements refers to tracing locations and paths; surveilling places refers to installing surveillance equipment in places where there may be evidence or facts of a crime.⁵³ When public security agencies adopt technical investigative measures, relevant entities and individuals, including service providers, have the obligation of cooperating with those public security organisations (paragraph 4 of Article 152 of the CPL). Because of their secrecy, technical investigative measures can be a serious threat to individuals' privacy and freedom of communication.⁵⁴ Therefore, even though not explicitly required by the CPL, the complementary principle⁵⁵ for technical investigative measures can be derived from the following rules established in the law to limit their usage.

⁵³ Liu Meixiang, 'Empirical Study on Supervisory Technical Investigative Measures' (2019) 4 *ECUPL Journal* 99 (in Chinese).

⁵⁴ Zhang Jianwei, 'The Procedure Specification and Information Processing of Technical Investigation', *Procuratorate Daily*, 4 July 2012, 3 (in Chinese).

⁵⁵ The complementary principle for technical investigative measures is also recognised as the last resort principle, meaning that technical investigative measures will be used only when other investigative measures do not work. Wang Dong, 'On Legal Regulations for Technical Detection' (2014) 5 *China Legal Science* 274 (in Chinese).

Firstly, technical investigative measures can be carried out only after the case is put on file and only to investigate the following crimes: crimes endangering state security, crimes of terrorist activities, organised crimes committed by groups in the nature of criminal syndicates, serious drug-related crimes or other crimes seriously endangering society, serious crimes where state personnel take advantage of their power to gravely infringe upon the personal rights of citizens (Article 150 of CPL) and serious duty-related crimes such as corruption and bribery (Article 28 of the Oversight Law). In pursuit of a fugitive criminal suspect or a fugitive defendant who is on the wanted list, or whose arrest has been approved or decided, necessary technical investigative measures may also be employed.

Secondly, technical investigative measures can be employed only after going through stringent approval procedures. To investigate crimes endangering state security, crimes of terrorist activities, organised crimes committed by groups in the nature of criminal syndicates, serious drug-related crimes or other crimes seriously endangering society, the competent authorities to employ technical investigative measures are the public security agencies at or above the municipal level (Article 150 of the CPL and Article 264 of the Provisions PSA). A report to require technical investigative measures must be sent to the principal of the public security organisation at or above the municipal level for approval (Article 265 of the Provisions PSA). If approved, an order adopting technical investigative measures will be issued and will be valid for three months (Article 151 of the CPL).

17.4.2.3 Comments on the Electronic Data Collection Procedure and Its Effects on the Cooperating Service Provider

Over the past decade we have observed the evolution of the regulations concerning collection of electronic evidence and technical investigative measures, seeking to restrict their application and protect personal privacy and freedom. However, there is still room for improvement. The following are some problems frequently discussed concerning electronic evidence collection procedures, which in some way cause difficulty for service providers in cooperating and are in conflict with service providers' mandate to protect customers.

The most significant problem is the procedure of electronic data collection. As introduced in Section 17.4.2.1, the Provisions PSA, the Rules MPS and the Joint Provisions all focus on different measures to be applied in the collection of electronic evidence, with little concern about the sensitivity of data or the degree of intrusiveness of certain measures. In the future, specific procedures should be designed based on a balance of crime investigation and human rights protection, especially the rights of privacy. As pointed out by some scholars, different types of electronic data must be collected via different procedures.⁵⁶ Content data and other data that is highly related to users' correspondence and privacy, namely the subjects of emails and information from big data that reflects personal lifestyle or daily routine, require a higher collection threshold and more procedural protections.⁵⁷ By applying some intrusive collection measures, we may need extra preconditions, for example to limit the application of certain

⁵⁶ Zhou Jiahai and Yu Haisong, 'The Interpretation and Application of the Provisions on Several Issues Concerning the Collection, Taking, Examination and Judgement of Electronic Data in the Handling of Criminal Cases' (2017) 28 *People's Judicature (Application)* 32 (in Chinese).

⁵⁷ Pei Wei, 'Internet Service Provider's Obligation of Disclosing Clients' Data During Criminal Investigation: From the Perspective of the Principle of Proportionality' (2016) 4 *Journal of Comparative Law* 103 (in Chinese); Pei Wei, 'Boundaries of ISP's Obligation in Assisting Law Enforcement: From the Perspective of Personal Data Protection' (2018) 1 *Journal of Cyber and Information Law* 46-47 (in Chinese).

collection procedures to more serious cases or to require approval from entities other than the investigative agencies.

The second problem concerns the principles of proportionality and data minimisation when coordinating concrete methods of electronic data collection. In China, seizure of the original storage media is ranked as the highest priority among all data collection methods.⁵⁸ As long as seizure of the original storage media is possible, it has to be conducted (Article 10 of the Rules MPS); only when seizure of the original storage media is not possible can the data be extracted (Article 9 of the Joint Provisions). This hierarchy may exist in consideration of the fact that seizure of the original storage media is a thorough preservation of all the information carried on it, including content information and system environment information, in order to prevent the electronic data from being deleted or altered.⁵⁹

However, seizure of the original storage media when collecting electronic evidence may not always be necessary. Unlike traditional documentary evidence where you have to keep its physical form to maintain the integrity of the evidence, electronic evidence can be copied or extracted without taking its original storage devices and without destroying its evidentiary value.⁶⁰ Moreover, seizure may not be always appropriate, for the reason that seized original storage media often contain far more data besides the electronic data that would serve as evidence.

Thus, it is no wonder that such an investigation priority may cause conflicts with the principle of proportionality or data collection minimisation in legal practice. Paragraph 1 of Article 141 in the CPL establishes that all property and documents found during an investigation that may prove a criminal suspect's guilt or innocence must be sealed up or seized, except for property and documents that are irrelevant to the case. Article 4 of the Rules MPS also provides that any material obtained that is irrelevant to the case must be returned or destroyed in a timely manner. A widely discussed case related to seizure of original storage media is the case of QvodPlayer suspected of spreading pornography for profit in 2013.⁶¹ QvodPlayer rented four servers from Beijing Wanglian Guangtong Technology Company. All four servers were seized in the later investigation because the investigators could not merely take the electronic data relevant to the case on the spot within a short period. The servers had a total capacity of 40 TB, among which only 29,841 videos were extracted and 21,251 videos were identified as pornographic.⁶² The seizure obviously infringed the principle of proportionality.

The third problem regarding electronic data collection is the lack of differentiation from traditional evidence, disregarding the special nature of electronic evidence. Taking the seizure of emails as an example, as introduced in Section 17.4.2.1.3, the email seizure procedure imitates the traditional mail seizure procedure, leaving out the dissimilarity between traditional paper-based mail and email. Nowadays the electronic data in an email is reproducible and under the control of email service providers, so it is not difficult for the police to get a copy of an email from a service provider, without the knowledge of the email owner. Therefore, the procedure of email

⁵⁸ Pan Jingui and Li Guohua, 'The Electronic Evidence Collection Methods' Interference in Basic Rights and Their Improvements of Legislation' (2019) 5 *Social Sciences in Hunan* 75 (in Chinese).

⁵⁹ Chen Yongsheng, 'On Construction of Electronic Communication Data Search and Seizure System' (2019) 1 *Global Law Review* 16 (in Chinese).

⁶⁰ Pei Wei, 'On the Seizure of Media in Criminal Electronic Evidence Collection' (2020) 4 *Criminal Science* 6 (in Chinese).

⁶¹ Criminal Final Instance of Beijing, First Intermediate Court of 2016 [(2016) Beijing 1 Criminal Final No. 592].

⁶² Xie Dengke, 'An Analysis of Electronic Data and the Revolution of Criminal Proceedings from the Perspective of the QvodPlayer Case' (2018) 5 *Oriental Law* 49 (in Chinese).

seizure should be designed in a workable way given its electronic features and provide more protection to the email owner or the suspect.

Lastly, regarding the regulations of electronic data collection, as presented in Sections 17.4.1 and 17.4.2.1, the CPL includes only very abbreviated and ambiguous provisions concerning the collection of electronic evidence and the cooperation obligations of all persons and entities, including service providers. Therefore, the main legal resources of collecting electronic data rely unreasonably and disproportionately on supplementary legal documents, including the Provisions PSA, the Rules MPS and the Joint Provisions. To meet the need of electronic data collection in reality, instead of merely serving as guidelines for or further explanation of the investigative methods that already exist in the CPL, these documents created some new investigative methods that are not regulated in the CPL, and some of the methods are quite intrusive in nature. For example, extracting electronic data on site or online and freezing electronic data (from Article 16 to Article 40 in the Rules MPS; see earlier in Section 17.4.2.1) are the two methods that were created in the aforementioned supplementary legal documents, and their legality cannot be justified because of the lack of root provisions in the CPL.

17.4.3 *Electronic Evidence Collected in Administrative Proceedings to Be Used in Criminal Cases*

Besides the electronic evidence collected in criminal proceedings, the physical evidence (including electronic evidence) obtained by administrative agencies may also be submitted to criminal proceedings as evidence. In accordance with paragraph 2 of Article 54 of the CPL, physical evidence, documentary evidence, audiovisual materials, electronic data and other evidence gathered by administrative agencies during administrative proceedings (i.e. supervision or inspections and investigations resulting potentially in administrative sanctions) may be used as evidence in criminal cases. Therefore, in order to provide a better understanding of how electronic evidence can be introduced into criminal proceedings, it is necessary to discuss the main methods for administrative organisations to obtain electronic evidence and its admissibility in criminal cases.

17.4.3.1 Evidence Obtained in Administrative Proceedings via Cooperation by Service Providers

There are principally four types of cooperation obligations on service providers in administrative proceedings, namely: (1) monitoring and transmitting illegal data to the relevant authority (this may diverge from the principle in other countries that platforms take no responsibility for the content users publish or transmit); (2) submitting information upon the request of relevant administrative agencies; (3) keeping records for a certain period (discussed earlier in Section 17.2.2) and storing data within the territory of China (to be discussed in Section 17.5.2); and (4) complying with a real name registration obligation requiring users to provide real identity information. The details of these obligations vary from one type of service to another.

17.4.3.1.1 MONITORING AND TRANSMITTING ILLEGAL DATA. In principle, service providers take no responsibility for illegal information sent by users. But, with the increasing role the internet plays in people's lives, the laws and regulations, especially in the administrative field, have created exceptions under certain circumstances for certain types of service providers, typically news information service providers (Article 16 of the Provisions for the Administration of Internet

News Information Services), internet forum and community service providers (Article 7 of the Provisions on the Administration of Internet Forum and Community Services)⁶³ and comments posting service providers (Article 4 of the Provisions on the Administration of Internet Comments Posting Services).⁶⁴ When discovering the transmission of illegal information,⁶⁵ service providers must immediately cease the transmission, preserve relevant records, delete relevant information and report the event to the relevant authorities.⁶⁶

17.4.3.1.2 SUBMITTING INFORMATION UPON THE REQUEST OF ADMINISTRATIVE AGENCIES. Furthermore, service providers in China are also under an obligation to cooperate at the request of relevant administrative agencies, besides police and prosecutors. There are mainly two types of requests.

The first one consists in providing information. For example, the E-commerce Law⁶⁷ provides that e-commerce business operators must produce e-commerce data and information when relevant authorities require them to do so in accordance with laws or administrative regulations (Article 25 of the E-commerce Law).

The second type of request is to cease the transmission of and delete the illegal information. Certain departments of the government have the authority to supervise the information on the internet; when discovering illegal information related to their authority, they will request the service providers to take action, including preserving the relevant records and providing assistance in the investigation.

17.4.3.1.3 REAL NAME REGISTRATION OBLIGATION. Since 2012, businesses that provide network access and domain name registration services, that handle stationary or mobile phone network access or that offer information publication or instant messaging services must require users to provide real identity information at the moment of signing the agreement or when confirming the provision of services. Users that do not register in their real name will not be offered full service.

17.4.3.2 Collection Requirements and Admissibility of Electronic Evidence

For now, no general provisions on electronic data collection – from any laws or regulations – are universally applied to all administrative proceedings. The provisions are scattered over various administrative laws and regulations. For the public security organisation, since it has both criminal and administrative investigative powers, the collection of electronic evidence in both proceedings basically follows the same requirements.⁶⁸ Other administrative laws and regulations set even

⁶³ Provisions on the Administration of Internet Forum and Community Services (Provisions AIFCS), 25 August 2017, Art. 16, www.cac.gov.cn/2017-08/25/c_1121541921.htm (in Chinese).

⁶⁴ Provisions on the Administration of Internet Comments Posting Services (Provisions AICPS), 16 November 2022, Art. 4, www.cac.gov.cn/2022-11/16/c_1670253725725039.htm (in Chinese).

⁶⁵ In general, the following three types of information are considered illegal: information that endangers national security and public interest; information that infringes private rights; and information that breaks public order and good morals (Cybersecurity Law, Art. 12). The exact range of illegal information may be slightly different depending on the applicable law or regulations.

⁶⁶ The procedure may vary depending upon the applicable law or regulations. For example, the Administrative Measures for Internet Information Services do not explicitly require the deletion of illegal information, while the Counterterrorism Law does.

⁶⁷ E-commerce Law, 31 August 2018, www.npc.gov.cn/zgrdw/npc/lfzt/rlyw/2018-08/31/content_2060834.htm (in Chinese).

⁶⁸ See, e.g., Provisions on the Procedures for Handling Administrative Cases by Public Security Organisations (Provisions HACPSO), 6 August 2020, Art. 32, www.nia.gov.cn/News/new/content.jsp?id=1460750 (in Chinese). The Provisions were first issued in 2012 and amended in 2014, 2018 and 2020. The discussion here focuses on the 2020 version.

higher standards for electronic data collection. For example, in accordance with Article 4 of the Guiding Opinions of the State Administration for Industry and Commerce on Collection of Electronic Data Evidence by Administrations for Industry and Commerce,⁶⁹ electronic evidence must be collected in the presence of at least two law enforcement officers, and at least one officer must have expertise with computer systems. This contrasts with the Joint Provisions and the Rules MPS, which do not specify the qualifications of the investigators.

It is important to highlight that there have been several criminal cases where electronic data collected by administrative authorities was not accepted by the court.⁷⁰ As provided by Article 54 of the CPL, evidence collected in administrative proceedings may be excluded because of its potential substantial damage to due process rights.⁷¹ The government is now constructing information-sharing platforms among administrative authorities, police, prosecution offices and courts, so that the electronic data collected by administrative authorities can be safely stored and conveniently transmitted to the criminal proceedings.⁷²

17.4.4 *Responsibility for Failure to Cooperate*

The cooperation obligations for service providers are, both in administrative proceedings and in criminal investigations, mandatory in nature. Failure to fulfil those cooperation obligations will result in administrative sanctions or even criminal liability.

17.4.4.1 Administrative Sanctions for Failure to Fulfil Cooperation Obligations

Service providers are obliged to cooperate with the police in administrative proceedings and criminal investigations. Failure to do so will lead to administrative sanctions. These sanctions are primarily laid down in Articles 61, 68 and 69 of the Cybersecurity Law, Article 48 of the Data Security Law and Article 84 of the Counterterrorism Law. Other regulations, such as the Administrative Measures for Internet Information Services,⁷³ the Provisions on the Administration of Internet Audio-Visual Program Service⁷⁴ and the Interim Provisions on the Administration of Internet Culture, also contain sanctions for failure to fulfil the administrative obligations therein provided. The administrative sanctions usually include an order for correction, a suspension or termination of operations, administrative fines and even detention of the director and the responsible personnel.

⁶⁹ Guiding Opinions of the State Administration for Industry and Commerce on Collection of Electronic Data Evidence by Administrations for Industry and Commerce, No. 248, 12 December 2011, Art. 4, www.waizi.org.cn/law/11557.html (in Chinese).

⁷⁰ See Pei Wei, 'The Connection of the Electronic Forensics Rules Before and After Criminal Recording: From the Perspective of Procedural Nature of Electronic Evidence' (2019) 2 *Contemporary Law Review* 115 (in Chinese).

⁷¹ See *ibid.*, 118.

⁷² See Liu Yong, 'Study on the Electronic Data Convergence Mechanism of Administrative Law and Criminal Law under the Background of Big Data' (2018) 5 *Administrative Law Review* 132–135 (in Chinese). The construction of information sharing platforms can be found in documents such as: State Council, Section Legislative Affairs, 'Opinions of Strengthening the Convergence Works of Administrative Legal Enforcement and Criminal Judiciary', 9 February 2011; and State Administration for Industry and Commerce, Ministry of Public Security and Supreme People's Procuratorate, 'Opinions on Several Issues of Strengthening the Convergence and Assistance Works of Industry and Business Administrative Legal Enforcement and Criminal Judiciary', 18 December 2012.

⁷³ Administrative Measures for Internet Information Services, 8 January 2011, www.gov.cn/zhengce/2020-12/26/content_5574367.htm (in Chinese).

⁷⁴ Provisions on the Administration of Internet Audio-Visual Program Service, No. 3, 28 August 2015, www.gov.cn/gongbao/content/2015/content_2975891.htm (in Chinese).

More in particular, Article 61 of the Cybersecurity Law provides sanctions for failure to fulfil the real name obligation. The competent department must order the service provider to take corrective action. If the latter fails to take corrective action or if the circumstances are serious, it shall be fined not less than 50,000 CNY but not more than 500,000 CNY, and the competent department may order it to suspend relevant business operations, cease business operations for rectification or close down the website, or it may revoke the relevant business permit or business licence, and impose a fine of not less than 10,000 CNY but not more than 100,000 CNY on its directly responsible person in charge and other directly liable persons.

Articles 68 and 69 of the Cybersecurity Law provide the sanctions for failure to monitor and transmit illegal data to the relevant authority and failure to submit information upon the request of relevant administrative agencies and failure to provide technical support and assistance to the police or a state security authority; Article 48 of the Data Security Law provides sanctions for failure to cooperate with the police or a state security authority when investigating crimes or maintaining national security. The sanctions are similar to those in the aforementioned Article 61 of the Cybersecurity Law.

Article 84 of the Counterterrorism Law encompasses sanctions for failure to provide technical interface, decryption and other technical support and assistance for the prevention and investigation of terrorist activities conducted by the police or a national security authority as required; or failure to cease the transmission and deletion of information with any terrorist or extremist content, preserve the relevant records, shut down the relevant website or terminate provision of the relevant services according to the requirements of the competent department; or failure to implement network security, information content supervision rules or technical measures for security prevention, which causes the dissemination of information with any terrorist or extremist content and the circumstances are serious. The competent department shall impose a fine of not less than 200,000 CNY but not more than 500,000 CNY on the violator, and impose a fine of not more than 100,000 CNY on its directly responsible persons in charge and other directly liable persons; if the circumstances are serious, it shall impose a fine of not less than 500,000 CNY on the violator, and impose a fine of not less than 100,000 CNY but not more than 500,000 CNY on its directly responsible persons in charge and other directly liable persons, and the public security authority may detain its directly responsible persons in charge and other directly liable persons for not less than five days but not more than fifteen days.

Before deciding to impose sanctions, the competent administrative department usually has a disciplinary interview with non-cooperative service providers. This disciplinary interview works as a soft method to promote service providers' cooperation. Indeed, it is an essential tool of the Chinese government to supervise and control the internet before formal sanctioning, helping to make up for the lack of law enforcement resources, to clarify service providers' obligations case by case and to urge service providers to meet their obligations.⁷⁵

17.4.4.2 Criminal Liability for Failure to Fulfil Cooperation Obligations

In addition to the aforementioned administrative sanctions, failure to fulfil cooperation obligations may also result in criminal liability. In case of non-cooperation, service providers can be prosecuted for the crime of 'refusing to perform the information network security management

⁷⁵ Lu Chao, 'The Research on Administrative Negotiation Tool in China's Internet Content Regulation' (2019) 2 *Chinese Public Administration* 42-44 (in Chinese).

obligation' provided in Article 286-1 of the Criminal Law as amended in 2015. A conviction of this crime requires all of the following elements:

- (1) the service provider has 'obligations for security management of information networks' as prescribed by laws and administrative regulations, but fails to meet these obligations;
- (2) it refuses to correct its acts as ordered by the competent authorities; and
- (3) the refusal causes serious consequences, such as spread of a large amount of illegal information, serious loss of evidence for a criminal case or leakages of users' information that lead to serious results.

Whoever is guilty of this crime shall be sentenced to a fixed-term imprisonment of not more than three years, criminal detention or public surveillance and concurrently or separately fined. Where an entity⁷⁶ commits the crime, it shall be fined. The director and other responsible personnel shall also be punished.

In the above offence definition, the wording of 'security management obligations regarding information networks' caused broad discussions about the source of these obligations, but the Cybersecurity Law is without doubt considered one such source.⁷⁷ Since Article 28 of the Cybersecurity Law imposes a cooperation obligation for service providers in criminal investigations (explained in Section 17.4.1), failure to cooperate may lead to the application of Article 286-1 of the Criminal Law.

Given that security management obligations regarding information networks cover a rather wide range, Article 286-1 of the Criminal Law has been criticised for being overly broad. Scholars suggest that this legislative wording should be interpreted more strictly to avoid overcriminalisation.⁷⁸ On the other hand, in judicial practice, convictions for the crime of Article 286-1 turn out to be surprisingly rare.⁷⁹ From 2015 to 2020, there were only two criminal cases of this crime,⁸⁰ neither of which resulted in a conviction. This crime is punishable only when the service providers refuse to correct when they receive the correction order from the administrative agencies. Typically, service providers opt to correct in order to avoid possible criminal prosecution and punishment. That is why, in judicial practice, very few service providers are prosecuted.⁸¹

One of the most recent and remarkable cases is the *Didi* case in Yueqing City (located in Zhejiang Province), in which non-cooperation of the service provider caused a victim's death

⁷⁶ 'Entity' here refers to a company, enterprise, institution, organisation or group which commits an act endangering society that is considered a crime under the law and shall bear criminal responsibility as a whole. See, e.g., Criminal Law, Art. 30.

⁷⁷ Some experts suggest that the source could include some, but not all, administrative regulations that impose obligations on service providers, but others focus purely on the Cybersecurity Law. See, e.g., Chen Hongbing, 'On the Application Space of the Crime of Failure to Perform the Information Network Security Management Obligation' (2017) 12 *Political Science and Law* 39–42 (in Chinese); Zhou Hongbo and Yue Xiangyang, 'How the Network Security Law Relates to the Criminal Law' (2018) 6 *Journal of Capital Normal University* 49–51 (in Chinese); Yang Xinlv, 'On the Legal Interests of Refusing to Fulfil the Obligation of Information Network Security Management Crime' (2019) 6 *Northern Legal Science* 46–47 (in Chinese); Pi Yong, 'On Service Providers' Management Obligations and Criminal Responsibilities' (2017) 5 *Studies in Law and Business* 23 (in Chinese).

⁷⁸ Pi, 'On Service Providers' Management Obligations', 24.

⁷⁹ Tong Dehua and Ma Jiayang, 'Justification and Research on the Types of the Obligations in Refusing to Fulfil the Obligation of Information Network Security Management Crime' (2020) 21 *Journal of Law Application* 80 (in Chinese).

⁸⁰ Ma Chaoyang and Ren Pengbin, 'Refusing to Fulfil the Obligation of Information Network Security Management Crime: Plight in Practice, Lawful Connotation and Thoughts of Responses', in *Theory and Practice of Cyberspace Crime Governance to Optimize Criminal Procuratorial Supervision: Collected Works of the 16th National Senior Prosecutors Forum* (Beijing: China Procuratorial Press, 11 November 2020) 2 (in Chinese).

⁸¹ Xiong Bo, 'On the Negativity of "Prior Administrative Procedure" for Criminal Liability of Network Service Providers and Its Solutions' (2019) 5 *Political Science and Law* 50 (in Chinese).

but did not constitute the crime of Article 286-1. Didi is the largest online ride-hailing platform in China. On 25 August 2018, the victim, a twenty-year-old girl, hitched a ride through Didi in the city of Yueqing. After getting into the car, she sent a text message to her friends asking for help. Her friends soon called the police. At 16:41 the police required Didi to provide more detailed information about the driver and his car twice, alleging that its security expert would intervene. Only an hour and a half later, at 18:13, did Didi send the car number and other information about the driver to the police.⁸² But it was too late, the girl had already been raped and killed by the driver.

Requiring to provide information is an investigative method in criminal procedure. Failing to provide the police with the requested information in time and thus failing to fulfil its cooperation obligation in the criminal investigation, Didi was punished administratively. Soon after the *Didi* case in 2018, the Ministry of Transport, the Ministry of Public Security and related agencies in Tianjin, Zhejiang and Beijing summoned senior executives of Didi for a disciplinary interview and ordered the company to rectify the problems with its online ride-hitching services. Didi was required to fulfil its security responsibility and cooperate with the public security agencies in future criminal cases.⁸³ Didi's Hitch Service was suspended for 435 days, the time taken for the company to modify and improve 330 functions of its service.⁸⁴

Since the Didi company did not refuse to make corrections, it did not commit an offence. This case clearly shows the limitations of Article 286-1 of the Criminal Law, which puts too much weight on administrative orders to make corrections. It only requires service providers to fulfil their obligations, correct illegal behaviours, eliminate adverse effects and restore property to its original condition. But obviously the right to life and health cannot always be restored.⁸⁵

17.4.5 *Legal Remedies and Protection of Fundamental Rights*

Legal remedies and protection of fundamental rights which relate to criminal investigations, especially the collection of electronic evidence, can be found in the following areas: notification of data collection; limited usage of data obtained; application procedure of data collection and complaints against unreasonable search and seizure; exclusion of illegally obtained evidence; and state compensation for the damages caused by improper investigative measures. Some of these remedies and protections are quite successful, but others are still rather vague and their effects are limited in practice.

17.4.5.1 Notification of Data Collection

Articles 17 and 18 of the PIP Law impose general notification obligations on service providers: before processing personal information, service providers must notify individuals of, among other matters, the purposes and methods of processing of personal information, the categories of

⁸² Public Security Bureau of Wenzhou City, 'A Report about the Work of Police after the Alarm Received in the Homicide Case of Didi Driver in Yueqing City', *Safe Wenzhou*, 25 August 2018, https://mp.weixin.qq.com/s?__biz=MjM5ODEzNDZMw==&mid=2652325164&idx=1&sn=0acdb748b810c6710521cd9f43ebb67c (in Chinese).

⁸³ Zhao Wenjun and Qi Zhongxi, 'The Ministry of Transport, the Ministry of Public Security and Related Agencies Summoned Didi for Face-to-Face Meeting', *Xinhua News*, 26 August 2018, www.gov.cn/xinwen/2018-08/26/content_5316759.htm (in Chinese).

⁸⁴ Qin Jing and Du Gang, 'Didi's Hitch Service Coming Back to Seven Cities, Can Passengers Travel at Ease?', *Xinhua News*, 8 November 2019, <http://travel.people.com.cn/11/2019/1108/c41570-31444346.html> (in Chinese).

⁸⁵ Xiong, 'On the Negativity', 55.

personal information to be processed and the retention periods, unless laws or regulations provide that such processing shall be kept confidential or that notification is not necessary.

However, there is no explicit provision on notification to suspects when the police collect data from a service provider, which often takes place without suspects' knowledge. Thus, a suspect's right to be notified about the information collection and its procedure is not guaranteed. On the contrary, in many cases the processing is kept confidential.

17.4.5.2 Limitation on the Usage of Collected Data

According to Article 152 of the CPL, investigators must promptly destroy any information and materials obtained using technical investigative measures that are irrelevant to the case. Moreover, materials obtained through technical investigative measures must be used only for the investigation, prosecution and trial of specific cases, not for any other purposes. Relevant entities and individuals must cooperate with public security agencies in their application of technical investigative measures in accordance with the law and must keep confidential all relevant information.

The Joint Provisions and the Rules MPS also require that the original storage media that have been sealed up or seized, or the frozen electronic data, must be freed within three days after they are found to be irrelevant to the particular case under investigation (Article 12 of the Joint Provisions, Articles 22 and 38 of the Rules MPS).

17.4.5.3 Data Collection Approval and Complaint Procedures

As was explained in Section 17.4.2, to protect fundamental rights, some electronic evidence collection methods that are particularly intrusive must be approved by a higher level of public security organisation.⁸⁶ Employment of technical investigative measures must be approved by public security agencies at or above the municipal level, and freezing of electronic data and seizure of email must be approved by public security agencies at or above the county level, whereas the director of the case-handling department has the power to approve requesting relevant entities and persons to provide electronic data. For other electronic data collection methods, the laws and regulations do not specifically provide the authority to approve, even though some of the methods also interfere with fundamental rights. It is important to highlight that there is no judicial warrant requirement for investigative measures (not even for the most intrusive ones) in criminal investigations in China. Therefore, the requirement to be approved by the principal of the public security organisation at the municipal or county level or above is already the highest-level protection available.

If suspects or service providers, as well as other interested parties, are of the opinion that the seal, seizure or freeze of property is irrelevant to the case at hand, or should have been terminated, they are entitled to file a petition or complaint to the police, the prosecution office or the judge, depending on which stage the case is at (Article 117 of the CPL). The organisation that accepted the petition or complaint must make a decision within thirty days and rectify the illegal sealing, seizure or freezing (Article 196 of the Provisions PSA). All aforementioned petitions and complaints apply to all kinds of property under sealing, seizure or freezing, not specifically electronic evidence.

⁸⁶ See, e.g., Jiang Yong, 'Procedural Law Turn of Electronic Investigation Regulation in China from the Perspective of Personal Information Protection' (2019) 6 *Journal of Xi'an Jiaotong University (Social Sciences)* 143–144 (in Chinese).

17.4.5.4 Exclusion of Illegally Obtained Evidence

Article 56 of the CPL establishes exclusionary rules of illegally obtained evidence. However, there is an absolute exclusion when it comes to testimonial evidence, including confessions extorted from a criminal suspect or defendant by illegal means such as torture, as well as the testimony of witnesses and statements of victims that are collected by violent means, threat or other unlawful means. The CPL does not preclude all of the illegally obtained physical or documentary evidence. Such evidence is admissible if it is not likely to cause substantial damage to due process and if the irregularity can be corrected in a reasonable way or can be justified by reasonable explanation. However, it is not clear whether the exclusionary rules can be applied to electronic evidence that is illegally collected.⁸⁷

Even if the judge accepts that the exclusionary rules can be applied to electronic evidence, there are only a few standards to apply when examining the legitimacy of the collection of electronic evidence. The Interpretation by the Supreme People's Court Regarding the Application of the Criminal Procedure Law (ICPL)⁸⁸ provides standards to apply when examining electronic data collected in criminal procedures,⁸⁹ including: whether the collection of electronic data is performed by two or more investigators; whether the collection methods are in compliance with relevant technical standards; and whether strict approval formalities are completed (Article 112 of the ICPL). But these standards focus more on guaranteeing the authenticity of electronic data, rather than the legality of its collection.⁹⁰ When electronic data is collected without the signatures or seals of investigators, it is not admissible unless it can be reasonably explained with a rectification of signature by the holders, the providers of the electronic data or eyewitnesses on transcripts or lists. Other than this, there are no provisions concerning the admissibility of illegally obtained electronic evidence in the ICPL.

17.4.5.5 State Compensation

Article 18(1) of the Law on State Compensation⁹¹ allows service providers whose original storage media are unlawfully sealed or seized during criminal investigations to apply for state compensation. The organisation liable for compensation is the authority in charge of the criminal investigation (Article 21 of the Law on State Compensation). To claim compensation, a service provider must first apply to the public security organisation responsible for the criminal investigation (Article 22 of the Law on State Compensation). The service provider may apply for reconsideration of the organisation's decision to the public security organisation at the next higher level or seek a decision from the compensation committee of the court (Articles 24 and 25 of the Law on State Compensation). If the original storage media can be returned or its original condition can be restored when damaged, this will be done. If the media cannot be returned to their original condition or are missing, compensation will be paid (Articles 32 and 36 of the Law on State Compensation).

⁸⁷ Zhang He, 'Study on the Rules of Illegal Electronic Data Examination in Criminal Procedure' (2021) 2 *BFSU Legal Science* 57 (in Chinese).

⁸⁸ Interpretation by the Supreme People's Court Regarding the Application of the Criminal Procedure Law (ICPL), 26 January 2021, www.court.gov.cn/fabu-xiangqing-286491.html (in Chinese).

⁸⁹ Joint Provisions also provide the standard to examine electronic data for legitimization in Article 24, and the provision has been absorbed into Article 112 of ICPL, so here we discuss only Article 112.

⁹⁰ Xie Dengke, 'On the Protection for Rights in Electronic Data Collection' (2020) 12 *Lanzhou Academic Journal* 44 (in Chinese).

⁹¹ Law on State Compensation, 26 October 2012, Art. 18(1), www.spp.gov.cn/sscx/201404/t20140424_71280.shtml (in Chinese).

17.5 CROSS-BORDER COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

17.5.1 Introduction

In 2020, during the Internet Development Forum of the World Internet Conference, the Ministry of Foreign Affairs launched the Global Initiative on Data Security,⁹² relating data security and governance of data to the issue of sovereignty, national security and jurisdiction of the state. In the initiative, China calls on all states to join forces in forging a community with a shared future in cyberspace, featuring peace, security, openness, cooperation and order. Therefore, states should neither request their own domestic companies to gather data generated and obtained overseas nor obtain data located in other states through companies or individuals without the other states' permission. Instead, they should obtain overseas data through mutual legal assistance. The initiative was considered a response to the Clean Network program put forward by the Trump administration in the United States.⁹³

In 2022, China submitted *Suggestions on the Scope, Objectives and Structure (Elements) of the United Nations Conventions on Countering the Use of Information and Communications Technologies for Criminal Purposes*⁹⁴ to the Ad Hoc Committee in the first session to elaborate the Convention as decided in Resolution 75/282 of the General Assembly of the United Nations in 2021. In these *Suggestions*, China reasserted its position as shown in the Global Initiative on Data Security, calling on the member states to respect the sovereignty of the state where the evidence is located, to abide by due process, to respect the legitimate rights of relevant individuals and entities and to take no invasive and destructive technical investigation means in cross-border electronic evidence collection.

Based on cyberspace sovereignty and data sovereignty, China has adopted a data localisation approach in deciding jurisdiction. Data localisation means that a state has the power to control and use electronic data stored within its territory. In Article 25 of the ICJA Law, electronic data is handled in the same manner as physical evidence. This illustrates that electronic data will be obtained similarly to physical evidence, and a territorial approach should be applied to decide its jurisdiction.⁹⁵

On the other hand, the PIP Law draws on the experience from the EU General Data Protection Regulation⁹⁶ and, for the first time, extends its application to personal information processing activities outside the territory of China on the principle of territoriality and personality.⁹⁷ Article 3 of the PIP Law states it applies to natural personal information processing activities within the territory of China as well as those outside the territory if they are for the purpose of providing products or services to natural persons located within China, or for

⁹² Ministry of Foreign Affairs, 'Global Data Security Initiative', 29 October 2020, www.mfa.gov.cn/wjlb_673085/zfxgk_674865/gknrlb/tywj/zcwj/202010/t20201029_9869292.shtml (in Chinese).

⁹³ Chaeri Park, 'Knowledge Base: China's "Global Data Security Initiative"', Digichina, 31 March 2022, <https://digi.china.stanford.edu/work/knowledge-base-chinas-global-data-security-initiative/>.

⁹⁴ *China's Suggestions on the Scope, Objectives and Structure (Elements) of the United Nations Convention on Countering the Use of ICTs for Criminal Purposes*, submitted by China as a member state of the United Nations on 5 November 2021, www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Chinas_Suggestions_on_the_Scope_Objectives_and_Structure_AHC_ENG.pdf.

⁹⁵ See Liang Kun, 'The Mode of Jurisdiction over Criminal Evidence Collection at the National Level Based on the Data Sovereignty' (2019) 2 *Chinese Journal of Law* 200 (in Chinese).

⁹⁶ Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, [2016] OJ L 119, 4 May 2016.

⁹⁷ Xu Yunfei, 'Interpretation of the Key Points in the Personal Information Protection Law', Weixin, 24 August 2021, https://mp.weixin.qq.com/s/KHDOXKRF5TPs_7tXR2KRVg (in Chinese).

the purpose of analysing or assessing the conduct of natural persons located within. Article 53 of the PIP Law further requires that personal information processors outside the territory of China shall establish special institutions or designate representatives within the territory of China to handle affairs relating to personal information protection, including cooperation with LEAs.

17.5.2 Mandatory Data Localisation Requirements

To guarantee data sovereignty and territorial jurisdiction, it is required that certain operators or service providers store certain types of data domestically. For now, there are mainly three types of operators and three types of data under the domestic storage obligation, as provided in the Cybersecurity Law, the PIP Law and the Data Security Law.

First, critical information infrastructure operators⁹⁸ shall store domestically the personal information or important data that is collected or generated during domestic operations (Article 37 of the Cybersecurity Law and Article 31 of the Data Security Law). ‘Domestic operations’ is defined as conducting business or providing products or services in the territory of China. Those service providers that do not register in China shall nevertheless be deemed to be conducting ‘domestic operations’ if they use the Chinese language or use the Chinese yuan (CNY) as currency or deliver goods or services to China.⁹⁹ In contrast, Chinese service providers that conduct business with or provide products or services solely to institutes, agencies or individuals outside of the territory of China shall not be deemed to be conducting ‘domestic operations’.¹⁰⁰ This type of data comprises only a small part of the data generated in the course of electronic commerce in China.¹⁰¹

Second, the PIP Law also provides that the personal information processors that process the personal information reaching the threshold specified by the national cyberspace administration in terms of quantity, as well as critical information infrastructure operators, shall store domestically the personal information collected and generated within the territory of China (Article 40 of the PIP Law). Despite the aforementioned strict data localisation requirement, it is still possible for certain data collected and generated domestically to be transferred across the border. If the data is deemed to be important, its cross-border transfer shall observe measures for security management developed by the national cyberspace authority in conjunction with the relevant departments of the State Council (Article 31 of the Data Security Law). For example, automobile data processors shall store important data domestically (Article 11). In this example, important data refers to data that may endanger national security, public interests or the lawful rights and

⁹⁸ Critical information infrastructures include public communication and information services, power, traffic, water resources, finance, public service, e-government and other critical information infrastructure which, if destroyed, suffering a loss of function or experiencing leakage of data, might seriously endanger national security, national welfare, the people’s livelihood or the public interest (Cybersecurity Law, Art. 31).

⁹⁹ Let’s take the example of Tesla Inc, an American multinational automotive and clean energy company that sells electric cars and provides services in China. In May 2021, Tesla set up a data centre in China to localise data storage; later that year, in September, the chief executive officer of Tesla promised at the World Internet Conference Wuzhen Summit that the personal identity information of the company’s Chinese clients would not be transferred abroad and that important data would be transferred abroad only after obtaining the approval of the competent authority in accordance with the Several Provisions on the Management of Automobile Data Security (see footnote 102). See, e.g., Xu Xu, ‘Tesla Promises No Cross-Border Transfer of Personal Identity Information’, China Economic Net, 26 September 2021, www.ce.cn/xwzx/gnsz/gdxw/202109/26/t20210926_36948364.shtml (in Chinese).

¹⁰⁰ Draft Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (draft for comments), 25 August 2017, Art. 3.2, www.tc260.org.cn/front/bzzqyjDetail.html?id=20170830211755&norm_id=20170221113131&rcode_id=23883 (in Chinese) (still has not been adopted).

¹⁰¹ Zhao Haile, ‘Data Localization in China’s Legislation and Its Reconciliation with FTA Conclusion’ (2022) 2 *Journal of International Economic Law* 30 (in Chinese).

interests of individuals or agencies when tampered with, destroyed, leaked or illegally obtained or used (Article 3).¹⁰²

Since the provisions that require domestic storage came into force, a number of high-tech companies and multinational corporations have already reacted. For instance, since 28 February 2018, Apple Incorporated has cancelled its cross-border storage for its iCloud services and built the first data centre in Guizhou Province, and now stores all the data of Chinese users in this data centre. Additionally, Apple has cooperated with the Guizhou-Cloud Big Data Industry Development Company to provide iCloud services to users in mainland China.¹⁰³

The domestic storage of data aims at protecting the data security of domestic users and it does help resolve some of the problems arising in the area of cross-border collection of electronic evidence.¹⁰⁴ On the other hand, it cannot resolve all of the problems, especially the problems of collecting data that is not covered by the requirement of domestic storage. It could also lead to an isolated information island, preventing timely and efficient collection of cross-border electronic data and development of an international mechanism for cross-border electronic data collection.¹⁰⁵

17.5.3 Cooperation of National LEAs with Foreign Service Providers

17.5.3.1 Legal Framework

As mentioned in Section 17.5.1, China's position is that collection of data located in other states through companies or individuals must be conducted with the permission of the state where the data is located. Therefore, the formal way to collect cross-border electronic data from international service providers still lies in mutual legal assistance.

This indirect cooperation (i.e. cooperation through mutual legal assistance) has long been criticised for low efficiency and incapacity to deal with changeable electronic data. An analysis shows that indirect cooperation is also rare. Research was conducted on a sample of thirty-five criminal cases that involved foreign servers, and illustrated that not a single piece of electronic evidence in these thirty-five cases was collected through mutual legal assistance. This is because the traditional mutual legal assistance approach is complex, slow and bureaucratic. Under such a procedure, it is difficult to respond efficiently to the flow of criminal data. Twenty-nine out of the thirty-five cases included the extraction of electronic evidence from foreign servers via open websites or via entering user name and password, while the collection method of the other six cases was not explicitly mentioned in the research report.¹⁰⁶

The Chinese police forces are seeking ways to promote the efficiency of traditional mutual legal assistance by simplifying the judicial assistance process and building sharing platforms for cross-border collection of criminal electronic evidence.¹⁰⁷ In 2019, the Office of Cooperation

¹⁰² Several Provisions on the Management of Automobile Data Security, issued by the Cyberspace Administration, the National Development and Reform Commission, the Ministry of Industry and Information Technology, the Ministry of Public Security and the Ministry of Transport (for Trial Implementation), No. 7, 16 August 2021, Art. 3, www.cac.gov.cn/2021-08/20/c_1631049984897667.htm (in Chinese).

¹⁰³ See Ren Xiaoyuan, 'The Apple Users' iCloud Will Move Back to Guizhou with Users' Privacy Promised by Apple', *Beijing Youth Daily*, 11 January 2018 (in Chinese).

¹⁰⁴ Feng Junwei, 'Development and Reflection of Cross-Border Obtaining Electronic Evidence' (2019) 6 *Law Science Magazine* 28 (in Chinese).

¹⁰⁵ See *ibid.*, 28.

¹⁰⁶ See Ye Yuanbo, 'Practical Investigation and Improvement of Cross-Border Electronic Forensics System in China' (2019) 11 *Hebei Law Science* 108 (in Chinese).

¹⁰⁷ Wang Zhigang and Zhang Xue, 'The Dilemma and Outlet of Cross-Border Electronic Data Forensics' (2021) 5 *Journal of Chongqing University of Posts and Telecommunications (Social Science Edition)* 51 (in Chinese).

and Coordination between China and Cambodia was founded in Phnom Penh, in which police and experts from the two countries work together and share electronic evidence collected.¹⁰⁸ This mechanism has proven successful in fighting crimes such as cross-border online gambling and telecom and online fraud.¹⁰⁹

Apart from mutual legal assistance between countries, there also exist attempts for LEAs to seek assistance directly from foreign service providers. However, an interview with the police revealed that it is difficult for national LEAs to directly obtain electronic evidence from foreign service providers, which are frequently unwilling to cooperate.¹¹⁰

17.5.3.2 Nature of the Cooperation

In accordance with Article 9 of the ICJA Law, where the case-handling organisation needs to request a foreign country to provide mutual legal assistance, it must prepare a written request for assistance with the relevant materials attached. After being examined and approved by the competent authority¹¹¹ to which the handling authority is subordinated, this request must be filed by the foreign affairs liaison authority in China with the foreign country in a timely manner.

The ‘foreign affairs liaison authority in China’ mostly refers to the Ministry of Justice, as provided in most treaties,¹¹² while the rest of the treaties designate the National Oversight Commission, the Supreme People’s Court, the Supreme People’s Procuratorate or the Ministry of Public Security as the foreign affairs liaison authority in China.¹¹³

17.5.3.3 Legal Remedies and Protection of Human Rights

For now, notwithstanding mutual legal assistance is slow and not very efficient, it is still the most common way for cooperation between national LEAs and foreign service providers to take place, in accordance with mutual legal assistance treaties between the states involved or through diplomatic channels. The treaties fully respect foreign countries’ sovereignty, and usually the gathering of evidence based on mutual legal assistance turns into a domestic issue on whether and how service providers need to cooperate with their national LEAs. In this sense, legal remedies and protection of human rights will strongly rely on the domestic laws of the service providers.

¹⁰⁸ Mao Pengfei, ‘The Office of Cooperation and Coordination between China and Cambodia Officially Founded in Phnom Penh’, Xinhua Net, 28 September 2019, www.gov.cn/xinwen/2019-09/28/content_5434513.htm.

¹⁰⁹ Ministry of the Public Security, ‘The Sum-Up Meeting for the Year of Legal Enforcement Cooperation between China and Cambodia Held’, National Immigration Administration, 4 June 2021, www.nia.gov.cn/n897453/c1415848/content.html.

¹¹⁰ See Feng, ‘The Collection of Internet Evidence’, 37.

¹¹¹ ‘Competent authority’ refers to the highest rank of the case-handling organisations which enjoy investigative powers on criminal cases, namely the National Supervisory Commission, the Supreme People’s Court, the Supreme People’s Procuratorate, the Ministry of Public Security, the Ministry of State Security and some other relevant government departments (ICJA Law, Art. 6).

¹¹² For example, Treaty on Judicial Assistance in Civil and Criminal Matters between the People’s Republic of China and the Russian Federation, signed 19 June 1992, www.mfa.gov.cn/web/ziliao_674904/tytj_674911/200804/t20080408_7948028.shtml (in Chinese); Agreement on Mutual Legal Assistance in Criminal Matters between the People’s Republic of China and the United States of America, signed 19 June 2000, www.mfa.gov.cn/web/wjlb_673085/zfxgk_674865/gknrlb/tywj/tyqk/200912/t20091204_9277065.shtml (in Chinese); and Treaty on Judicial Assistance in Criminal Matters between the People’s Republic of China and Australia, signed 3 April 2006, www.mfa.gov.cn/web/ziliao_674904/tytj_674911/tyfg_674913/200804/t20080408_9867450.shtml (in Chinese).

¹¹³ Wang Aili (ed.), *The Interpretation of the Law of International Criminal Judicial Assistance of the People’s Republic of China* (Beijing: Law Press China, 2019), 34 (in Chinese).

17.5.4 *Cooperation of National Service Providers with Foreign LEAs*

As mentioned in Section 17.5.2, service providers must store domestically certain data collected within the territory of China. Furthermore, direct cross-border data transfer from national service providers to foreign LEAs is prohibited.

The ICJA Law, adopted in 2018, prohibits institutions, agencies or individuals within the territory of China from providing evidentiary material and assistance prescribed by this Law to foreign countries without the approval of the competent authority of China (paragraph 3 of Article 4 of the ICJA Law). The PIP Law and the Data Security Law, both adopted in 2021, follow this position and specify that without the approval of the competent authority, a personal information processor or any domestic organisation or individual shall not provide personal information stored within the territory of China to any foreign judicial or law enforcement authority. All requests for data from a foreign judicial or law enforcement authority will be processed by the competent authority of China in accordance with the relevant laws and international treaties and agreements entered into or acceded to by China, or under the principle of equality and reciprocity (Article 41 of the PIP Law and Article 36 of the Data Security Law).

Where foreign LEAs need the cooperation of national service providers in China, they must make a request for mutual legal assistance, handing it to the foreign affairs liaison authority of China (Article 13 of the ICJA Law). The foreign affairs liaison authority will examine the written request and the attached materials, and forward them to the competent authority¹¹⁴ according to the division of functions (Article 15 of the ICJA Law). The competent authority will then examine the request. Where the competent authority deems that it may assist in the execution in accordance with the provisions of this Law and the mutual legal assistance treaty, it will make a decision and proceed to execution of the request by the relevant case-handling organisation (Article 16 of the ICJA Law). When executing a request, the case-handling organisation must protect the lawful rights and interests of the parties and other relevant persons, and protect personal information (Article 17 of the ICJA Law).

As the cooperation of national service providers with foreign LEAs follows the traditional mutual legal assistance method, it encounters the same problems of slowness and low efficiency as the cooperation of foreign service providers with Chinese LEAs. Another problem has arisen for multinational service providers. In March 2018, the US enacted the CLOUD Act, compelling US-based technology companies to produce requested data regardless of whether it is stored within or outside the US. To some extent, the prohibition of national service providers from providing evidence and assistance to foreign countries as regulated in paragraph 3 of Article 4 of the ICJA Law is China's response to the CLOUD Act.¹¹⁵ These laws are trapping service providers in a dilemma: when the US LEAs require US service providers that provide services within the territory of China or Chinese service providers that have branch offices in the US to provide electronic data, the service providers will have to follow the US LEAs' request or face punishment, while the Chinese Laws may prohibit them from doing so.¹¹⁶

¹¹⁴ According to Article 6 of ICJA Law, the National Oversight Commission, the Supreme People's Court, the Supreme People's Procuratorate, the Ministry of Public Security, the Ministry of State Security and other departments are the competent authorities in charge of international criminal judicial assistance. With regard to the collection of electronic evidence, it should be the agencies with investigative powers, including the National Oversight Commission, the Ministry of Public Security and the Ministry of State Security.

¹¹⁵ Hu Wenhua, 'The Impact of American CLOUD Act on China and Its Counter Measures' (2019) 7 *Information Security and Communications Privacy* 35 (in Chinese).

¹¹⁶ See, e.g., Liang, 'The Mode of jurisdiction', 206.

The cooperation between Chinese LEAs and foreign service providers, on the one hand, and between foreign LEAs and Chinese service providers, on the other, depends on traditional judicial assistance between both countries. Given its low efficiency and the aforementioned dilemma, China is now reflecting on adjusting its original data localisation position and clarifying electronic data jurisdiction boundaries. In the meantime, it is trying to strengthen the dialogue mechanisms with other countries to reach bilateral and multilateral agreements on the issue of cross-border data collection.¹¹⁷

China has firmly held the opinion that it is necessary to establish a universal or global legal instrument on cybercrime within the framework of the United Nations.¹¹⁸ In 2019 and 2021, the United Nations adopted Resolutions 74/247 and 75/282 to elaborate an international Convention on countering the use of information and communications technologies for criminal purposes. Supporting the elaboration on the Convention, China will ‘take a constructive part in the negotiation, and work closely with all parties to jointly push for an authoritative and universal convention at an early date, so as to provide a practical and effective solution for the international community to cope with the challenges of cyber crimes’.¹¹⁹

¹¹⁷ See Hu, ‘The Impact of American CLOUD Act’, 36; Liang Kun, ‘On the Change Logic of Terrorism Development Trend and Enlightenment of EU Cross-Border Fast Electronic Evidence System’ (2019) 1 *Journal of People’s Public Security University of China (Social Sciences Edition)* 40–42 (in Chinese).

¹¹⁸ Hu Jiansheng and Huang Zhixiong, ‘The Problems and Prospects of the International Legal Regimes in Combating Cybercrimes – From the Perspective of Council of Europe’s Convention on Cybercrime’ (2016) 6 *Chinese Review of International Law* 22 (in Chinese).

¹¹⁹ Ministry of Foreign Affairs of the People’s Republic of China, ‘Foreign Ministry Spokesperson Zhao Lijian’s Regular Press Conference on May 28, 2021’, 28 May 2021, www.mfa.gov.cn/eng/xwfw_665399/s2510_665401/2511_665403/202105/t20210528_9170754.html.

Cooperation of Service Providers in Criminal Investigations in the Russian Federation

Maria Filatova, Olga Kostyleva and Tatiana Alekseeva^{8*}

18.1 SETTING THE SCENE

18.1.1 *General Approach to the Collection of Digital Evidence*

The Russian law does not provide a definition of digital (or electronic) evidence or any particular rules in that respect. The Russian authorities take a pragmatic approach to collection of digital evidence, in practice. It can be done in several ways. One common method consists of an investigator having access to a suspect's computer during a search, simply opening the device, opening certain files and either making screenshots or just using his/her own smartphone to take pictures of the screen. In that case such screenshots and/or photos become the evidence. The other method consists of the investigator describing in a protocol what he/she sees on the screen and then the protocol becomes the evidence. Finally, it is also possible to hand the device to an expert for analysis and the expert's report will be used as evidence. It means that for digital evidence, the classic (traditional) forms of evidence gathering (search, seizure and expert opinion) are used for collecting the evidence, without taking into consideration the specifics of the digital features.

This approach is confirmed by the majority of the Russian doctrine. Accordingly, electronic evidence is not a special category of evidence but belongs to categories that already exist. The process of collecting evidence should then be focused on recording or safeguarding that piece of evidence, so that it can be used by an investigator or a judge.

However, that approach is not supported by all scholars. There are those who argue that it is necessary to draw attention to 'digital evidence' as a term and a concept.¹ They believe that it is necessary either to adapt traditional types of evidence to the digital reality or to provide new rules for gathering of e-evidence. Both points of view try to avoid the above-mentioned situations, in particular when the investigator uses photos taken by phones as evidence, instead of arranging for proper collection of data or seizure of a device. However, according to the existing law, the only

* The chapter was written with the assistance of Ivan Sukharev and Polina Nemchinova and a student research group of the Law Faculty of Moscow State University: Linda Davarskaya, Natalia Kirillova, Elizaveta Kazakova and Anastasiya Chernova.

¹ See, e.g., R. I. Okonenko, 'Elektronnyye dokazatel'stva kak novoye napravleniye sovershenstvovaniya rossijskogo ugolovno-protsessual'nogo prava' (2015) 3 *Aktualnyye problemy rossijskogo prava* 120–124. See also A. A. Tushev and N. A. Nazarov, 'Informatsiya kak osnova vseh vidov dokazatel'stv v ugolovnom protsesse' (2012) 3 *Obschestvo i Pravo* 195–197. They state that 'electronic evidence' is a special group within the already existing types of evidence, and therefore must be endowed with a special legal status, taking into account their characteristics. Disadvantages of criminal procedure provisions that do not allow forming a clear mechanism of obtaining information in a digital form are highlighted by N. A. Zigura and A. V. Kudryavtseva, *Kompjuternaya informatsiya kak vid dokazatel'stva v ugolovnom protsesse Rossii* (Moscow: Urlitinform, 2011).

other possibility would be to consider the phone of the perpetrator to be a piece of evidence. It would then, however, belong to the category of physical evidence, just like a knife with blood or a glass with fingerprints on it. Yet, this would not make much sense. Such physical evidence has probative value because of its *form*, not because of its content.² For example, if a document is important because there is blood of a victim on it, the document belongs to physical evidence. If its content is important – then it falls into the category of ‘documents’. Following that example, the phone of the investigator should fall into the last category, as the investigators and judges are interested exclusively in the content. Yet that is not possible according to the current Russian law.

Russian law contains a closed list of types of evidence. The list has not been amended in view of technological developments, but some modifications of concrete types of evidence were made. Several traditional criminal procedure provisions have been adapted to digital technologies. Examination (inspection) is usually used to record what an investigator sees on the screen of a device. A protocol of inspection becomes a piece of evidence as well as the device itself, but the device belongs to the group of physical evidence. Technical experts from the special police units are usually involved in this measure, in particular if technical expertise is necessary (e.g. if the phone is protected with a password). Expertise is another important investigative measure with a special legal nature.³ An expert’s opinion becomes a piece of evidence.

In order to work in the digital sphere, some changes to criminal procedure provisions were made. For example, Article 185 of the Code of Criminal Procedure regulates rules of search and seizure of postal and telegraph mail. This article was amended in 2016 and now allows applying these measures to messages in a digital form.⁴

In 2018 the general terms of investigation were also modified.⁵ An important new provision was introduced on electronic data storage devices. Those devices can be seized in certain cases enumerated by the law mainly concerning business (e.g. fraud, misappropriation of property, illegal enterprise and so on). The provision itself is aimed at protecting businesses that cannot operate without their devices and information. Seizure is possible when an investigator decides that the forensic examination of an electronic device is necessary; when there is a judicial order that allows it to be seized; when pieces of information stored on the device do not legally belong to a holder of the device and he/she is not empowered to store and use them; when information stored can be used to commit other crimes; or when copying information according to the view of a specialist may lead to its modification or destruction.⁶

² L. V. Golovko (ed.), *Kurs ugolovnoogo protsesssa*, 2nd ed. (Moscow: Statut, 2017), 520.

³ In regard to the investigative measure, an ‘expert’ should be distinguished from those experts that may help investigators in some activities. Expertise as an investigative measure means that there are some questions which are sent to the specific body which selects an expert to answer them. The result of the expertise is a piece of evidence, so it is not just technical assistance.

⁴ The way the norm was amended is criticised by scholars. For instance, some state that, in general, the legislator has chosen the correct way for development of criminal procedural legislation, as the rules that allow the law enforcement officer to receive a wide range of information are certainly necessary, but this provision was introduced by the legislator artificially, without a comprehensive legal and logical analysis. S. V. Suprun and V. S. Cherkasov, ‘O protivorechivom haractere novelly v zakonodatel’nom regulirovanii sledstvennogo dejstviya ‘nalozheniye aresta na pochtovo-telegraphnyye otravleniya’ (2017) 1(34) *Vestnik Omskoj juridicheskoy akademii* 59–64.

⁵ General terms of investigation apply to all kinds of evidence and exist alongside specific provisions on each kind of evidence. They contain norms on legal grounds of investigative measures, time when they can be carried out, some prohibitions and obligations of investigators and so on. See Federal’nyj zakon ‘O vnesenii izmenenij v stat’i 76.1 i 145.1 Ugolovnoogo kodeksa Rossijskoj Federatsii i Ugolovno-protsessual’nyj kodeks Rossijskoj Federatsii’ (Federal Law on Amending Articles 76.1 and 145.1 of the Criminal Code of the Russian Federation and the Code of Criminal Procedure of the Russian Federation), 27 December 2018, No. 533-FZ, Art. 2.

⁶ These conditions are broad enough to allow investigators to seize devices even in this category of cases. They are usually seized for a long period of time (until the end of hearing at court, so can last for years); that is why some authors suggest using cloud storages. See, e.g., D. V. Saushkin, D. D. Shul’gina and M. A. Korchagina, *Prava i obyazannosti*

The Code of Criminal Procedure also requires the participation of technical experts to work with information stored on electronic data storage devices and provides the opportunity to copy pieces of information, returning originals back to their holder. However, in practice the opportunity described is not an obligation of the investigator but is up to his/her discretion.⁷

The approach of adopting older procedural measures results in various problems affecting the human rights of affected persons. This can be illustrated by the example of mobile phones which have been seized and are being inspected. Despite the fact that mobile phones contain so many pieces of information on the private lives of their owners, courts interpret the existing rules as saying that a judicial order is not necessary to inspect the content of such devices.⁸ A judicial order is required only when the content of messages is transferred to law enforcement bodies by a third party (a service provider). Furthermore, the Constitutional Court of the Russian Federation confirmed that this practice is legal and constitutional.⁹ It seems to us that such an attitude to this investigative measure is against its nature as it interferes with the private life of the person involved without a proper legal basis.

18.1.2 Data Retention Obligations: Legal Framework, Practice and Challenges

The key federal law¹⁰ on data protection regulation does not contain a requirement to retain personal data, but it grants the right to data processors to retain data for the purposes related to their activity. Once it is no longer necessary in view of this activity, the processed data must be deleted or depersonalised within thirty days.

Having a clear purpose for retaining data is essential, but the data processors are relatively flexible in formulating them. Therefore, questionable judgments appear, such as the position of the Sverdlovsk Regional Court according to which processing data on traffic offences is lawful for security reasons even when the time has elapsed after which the persons concerned have the right to have their record cleaned.¹¹ This attitude is questioned because of its negative consequences for data subjects.¹²

For specific obligations on data retention, see Table 18.1.

Further obligations concern managers responsible for dissemination of information on the internet (information dissemination managers).¹³ Their obligations are described in the Federal Law on Information, Information Technologies and the Protection of

predprimatelya pri vzaimootnosheniyah s pravohranitel'nyimi organami: zakon i praktika (Moscow: Redaktsia 'Rossijskoj gazety', 2019), 139–143.

⁷ Investigators' decisions can be challenged in court if they interfere with constitutional rights and freedoms or if they block access to court. Decisions on electronic devices can be challenged as they interfere with rights of businesses.

⁸ It is the judicial interpretation of the general rule that a judicial order is necessary in case an investigative or operative-search measure interferes with constitutional rights. Classification of data on that ground is described in Section 18.2.1. Operative-search measures under our process are not investigative measures though they can be connected with criminal investigation. These two spheres are based on different principles (e.g. for operative measures, secrecy and conspiracy are extremely important).

⁹ General information on the Constitutional Court can be found here: www.ksrf.ru/en/Info/Pages/default.aspx. All executive and judicial bodies are bound by its decisions. See Konstitutsionnyj Sud Rossijskoj Federatsii (Constitutional Court of the Russian Federation), 25 January 2018, No. 189-O, para. 2.

¹⁰ Federal'nyj zakon o personal'nykh dannyx (Federal Law on Personal Data), 27 July 2006, No. 152-FZ.

¹¹ See, e.g., Sverdlovskij oblastnoj sud (Sverdlovsk Regional Court), 29 July 2015, No. 33-11645/2015.

¹² It refers to administrative offences and to crimes of all categories. People quite often state that such databases do not allow them to find a good job and interfere with their labour rights. Yet the courts still do not see it as a violation of any rights.

¹³ There can be a variety of possible translations of this term into the English language. Hereinafter we will use the term 'information dissemination manager' and in Section 18.2.2 there is a description of terms used for different agents in the sphere of data protection and communications and connections between those terms. There are many examples of information dissemination managers, such as VKontakte, WhatsApp, Skype, Gmail, Mail.ru and many others that provide opportunities to communicate via the internet for users.

TABLE 18.1 *Examples of data retention obligations*

What data?	By which data processors?	For how long?
Personal files of employees, work contracts	Employers	50 or 75 years*
Files of gaming participants	Gaming organisers	Not less than 5 years since the day participants were included in a database**
Credit records	Credit records bureau	7 years since the most recent change to a record***
Information on foreigners' arrival in Russia	Hotels	1 year†
Data on currency operations	Banks	Not less than 3 years since the operation was deregistered††

Notes: * Federal'noye Arkhivnoye Agentstvo (Federal Archive Agency), Prikaz 'Ob utverzhdenii perechnya tipovykh upravlencheskikh arkhivnykh dokumentov, obrazuyushchikhsya v protsesse deyatel'nosti gosudarstvennykh organov, organov mestnogo samoupravleniya i organizatsij, s ukazaniyem srokov ikh khraneniya' (Order on the List of Managerial Archive Documents, Related to Activities of Governmental Agencies, Municipal Bodies and Companies, and Duration of Their Storage), 20 December 2019, No. 236, para. 444.

** Pravitel'stvo Rossijskoj Federatsii (Russian Government), 'Pravila vedeniya v bukmekerskikh kontorakh i totalizatorakh ucheta uchastnikov azartnykh igr, ot kotorykh primimayutsa stavki, interaktivnyye stavki na ofitsial'nyye sportivnyye sorevnovaniya' (Rules on Registering of Game Participants Whose Bets on Sport Events Are Accepted by Betting Agencies and Gambling Systems), 14 August 2020, No. 1221, para. 5.

*** Federal'nyj zakon 'O kreditnykh istoriyakh' (Federal Law on Credit Records), 30 December 2004, No. 218-FZ, Art. 7, s. 1.

† Ministerstvo vnutrennikh del (Ministry of Internal Affairs), Prikaz (Order), 10 December 2020, No. 856, para. 103.

†† Bank Rossii (Bank of Russia), Instruksiya 'O poryadke predstavleniya residentami i neresidentami upolnomochennym bankam podtverzhdayushchikh dokumentov i informatsii pri osuschestvlenii valyutnykh operatsij, o yedinykh formakh ucheta i otchetnosti po valyutnym operatsiyam, poryadke i srokakh ikh predostavleniya' (On the Order of Submission of Documents and Information by Residents and Non-residents While Carrying Out Currency Operations, on Universal Forms of Reports, Deadlines and Order of Reports on Currency Operations), 16 August 2017, No. 181-I, para. 3.4.

Information.¹⁴ According to Article 10.1 of this Law, they carry out activities to ensure the functioning of information systems and/or programs for electronic computers, which are intended and/or used to receive, transmit, deliver and/or process electronic messages from users of the internet. This broad definition includes both legal and natural persons who operate on the internet using a service through which communications between internet users can be carried out.¹⁵ In practice, only legal persons are subject to these provisions.

Still, according to Article 10.1, information dissemination managers have to retain two kinds of data, metadata (or traffic data) and content data, for one year or for six months after the end of communication or processing, respectively. Metadata includes information on facts of transmissions, answers, processing of messages, texts, audio and video, pictures, voice messages between internet users and information on these users. Content data covers content of text messages, voice messages, pictures, and audio and video between internet users.

The obligations described above are binding not only for Russian companies but also for foreign ones processing the data of Russian users. In order to clarify whether a foreign company without a presence in Russia falls under Russian laws' obligation, enforcement agencies have

¹⁴ Federal'nyj zakon 'Ob informatsii, informatsionnykh tekhnologiyakh i o zaschite informatsii' (Federal Law on Information, Information Technologies and the Protection of Information), 27 July 2006, No. 149-FZ.

¹⁵ A. I. Saveliev, *Commentarij k Federal'nomu zakonu ot 27 ijulya 2006 g. No. 149-FZ 'Ob informatsii, informatsionnyh tekhnologiyah i zaschite informatsii' (postatejnyj)* (Moscow: Statut, 2015), 270–279.

begun to apply an approach inspired by private international law and legislation on the protection of consumer rights, based on whether the activities target the territory of the Russian Federation. A Russian-language version of the internet site, possibilities to make payments in rubles and/or to execute contracts concluded on such a website on the territory of the Russian Federation, and/or the use of advertising in Russian can prove that the business strategy of such an entity involves the Russian market.¹⁶

What is more, there is a separate Federal Law on the Activities of Foreign Persons on the Internet on the Russian Territory.¹⁷ According to its provisions, an entity is considered to be carrying out activities in Russia if more than 500,000 Russian users access its information systems or internet sites during a 24-hour period and, in addition to that, one of the four following criteria is met: (1) the entity processes personal data of Russian users; (2) it spreads/provides access to information in Russian or in another official language accepted by some entities of the federation, for example Tatar or Bashkir; (3) it places on its internet sites advertisements targeting Russian users; (4) it receives payments from Russian natural or legal persons. All these entities are enlisted in open access by the Roskomnadzor¹⁸ and include Google LLC; Twitter, Inc.; Discord, Inc.; Spotify Ab; and so on.¹⁹

Moreover, the same law lists some other categories of foreign entities which fall under its obligations regardless of the number of Russian users. Among them are information dissemination managers. While the Roskomnadzor does seem to pay attention to the number of users these categories of entities have (e.g. Roskomnadzor's online test to find out whether a company falls under the provisions of the law gives a negative answer if the number of users is fewer than 500,000).²⁰ However, the wording of the law does not consider this criterion as obligatory. The Register of those latter categories adds then to the list such providers as Threema GmbH; GLOBAL MICROTRADING PTE. LTD.; Badoo Trading Limited; Vimeo, Inc.; Snap Inc.²¹ As the number of Russian users can be irrelevant for entities which process electronic messages, they may also include, for instance, blogs. They are subject to Russian laws, but we believe that it is still necessary to prove that a Russian audience is actively targeted by the entity.

All foreign companies that meet any criteria of activities on the internet in Russia are obliged to establish an office in Russia or a Russian legal entity. Violations of this obligation lead to limits on advertisements or on receipts of payments from Russian users. The Roskomnadzor is also

¹⁶ These criteria are mentioned by the Ministry of Digital Development, Communications and Mass Media. See Ministerstvo tsifrovogo razvitiya, svyazi i massovykh kommunikatsij (Ministry of Digital Development, Communications and Mass Media), 'Otvet na chasto zadavayemye voprosy' (Frequently Asked Questions), 12 February 2016, https://digital.gov.ru/en/personaldata/?utm_referrer=https%3a%2f%2frppa.ru%2f.

¹⁷ Federal'nyj zakon 'O deyatel'nosti inostrannykh lits v informatsionno-telekommunikatsionnoj seti "Internet" na territorii Rossijskoj Federatsii' (Federal Law on the Activities of Foreign Persons on the Internet on the Russian Territory), 1 July 2021, No. 236-FZ.

¹⁸ The Roskomnadzor or Federal Service for Supervision of Communications, Information Technology and Mass Media is a federal executive body responsible for licensing and issuance of permits, as well as for control and supervision of telecommunications, information technology and mass communications. See Federal Service for Supervision of Communications, Information Technologies and Mass Communication (Roskomnadzor), 'Powers of Roskomnadzor', 29 January 2013, http://eng.rkn.gov.ru/about/powers_of_roskomnadzor/u. It holds a wide range of powers; among them it is responsible for protection of data subjects' rights.

¹⁹ Federal Service for Supervision of Communications, Information Technologies and Mass Communication (Roskomnadzor), 'List of Foreign Entities Operating on the Internet on the Territory of the Russian Federation', <https://236-fz.rkn.gov.ru/agents/list>.

²⁰ Roskomnadzor, 'Test to Identify the Foreign Entity', <https://236-fz.rkn.gov.ru/test>.

²¹ Roskomnadzor, 'Register of Information Dissemination Managers', <https://rkn.gov.ru/opendata/7705846236-InformationDistributor/data-20230105T0000-structure-20161206T0000.xml> or <https://97-fz.rkn.gov.ru/organizer-dissemination/viewregistry/>.

empowered to place a notice on their internet sites stating that such companies violate Russian legal provisions.²²

Liability for not complying with the duties of information dissemination managers is administrative. Offences include lack of notice to the Roskommnadzor, non-compliance with data retention obligations and obligations on cooperation with law enforcement agencies (LEAs) and are punished with fines for three types of offender – ordinary natural persons, executive officers and legal persons.²³

Pieces of information that must be retained are described in more detail by Resolution No. 1526 of the Russian Government of 23 September 2020. They include:

- user identification data;
- internet protocol (IP) address and time of registration;
- data the user reported while registered;
- data on the facts of authorisation;
- data on changes to and additions of personal data made by the user;
- data on commercial services provided for the user by the information dissemination manager;
- data on the end of being active on the internet;
- data on when and between whom messages were sent, received and processed; and
- data on money operations via the communication channel.²⁴

Another list of obligations applies to the category of communication providers.²⁵ They must also retain data on facts of transmissions, facts of sending, receiving and processing messages between users (i.e. traffic data), information on users (for three years since the end of communication/processing) and the content of all messages between users (for six months since the end of communication/processing).

Even if official reasons to provide these duties were to combat terrorism and organised crime,²⁶ these obligations are general and do not depend on offences or any categories of offences. Whether the data subject is a suspect or not, his or her data must be stored.

²² Federal'nyj zakon 'O deyatel'nosti inostrannykh lits v informatsionno-telekommunikatsionnoj seti "Internet" na territorii Rossijskoj Federatsii' (Federal Law on the Activities of Foreign Persons on the Internet on the Russian Territory), 1 July 2021, No. 236-FZ, Arts. 5, 9–10.

²³ Kodeks Rossijskoj Federatsii ob administrativnykh pravonarusheniyakh (Russian Code of Administrative Offences), 30 December 2011, No. 195-FZ, Art. 13.31.

²⁴ Russian Government, 'O Pravilakh khraneniya organizatorami rasprostraneniya informatsii v informatsionno-telekommunikatsionnoj seti "Internet" informatsii o faktakh priyoma, peredachi, dostavki I (ili) obrabotki golosovoj informatsii, pis'mennogo teksta, izobrazhenij, zvukov, video- ili inykh elektronnykh soobschenij pol'zovatelej informatsionno-telekommunikatsionnoj seti "Interne" i informatsii ob etikh pol'zovatelyakh i predostavleniya ee upolnomochennym gosudarstvennym organam, osushchestvlyayushhim operativno-razysknuyu deyatel'nost' ili obespechenie bezopasnosti Rossijskoj Federatsii' (Resolution on Information Storage Regulations by Information Dissemination Managers), 23 September 2020, No. 1526.

²⁵ Their role is defined in: Federal'nyj zakon 'O svyazi' (Federal Law on Communications), 7 July 2003, No. 126-FZ; Russian Government, 'Ob utverzhdenii Pravil vzaimodejstviya operatorov svyazi s upolnomochennymi gosudarstvennymi organami, osushchestvlyayushimi operativno-razysknuyu deyatel'nost' (Resolution on Approval of the Rules of Interaction of Communication Providers with Authorised State Bodies Engaged in Operational Investigative Activities), 27 August 2005, No. 538. See further on this category of providers in Section 18.2.2.

²⁶ Thus, the explanatory note of the bill highlights the aims of protection from terrorism and prevention of it. See Poyasnitel'naya zapiska k zakonoproektu 1039149-6 'O vnesenii izmenenij v otdel'nyye zakonodatel'nyye akty RF v chasti ustanovleniya doponitel'nykh mer protivodejstviya terrorizmu i obespecheniya obschestvennoj bezopasnosti' (Explanatory Note to Bill No. 1039149-6 On Amendments to Certain Legal Acts of the Russian Federation in Regard to Additional Measures to Combat Terrorism and Provide Security for Society), 7 April 2016, <https://sozd.duma.gov.ru/bill/1039149-6>.

In the first place, data subjects and data processors that process data with data subject consent have access to data.²⁷ The category of data processors is broad and includes all persons, legal persons and government bodies that process personal data, which means they may collect personal data and systematise, store, change, renew, use, transfer, delete, depersonalise or block it. The register of data processors is operated by the Roskomnadzor.

Apart from data subjects and data processors, access to personal data can be given to different categories of enforcement officers. They can be given access to certain kinds of metadata and content data only after a judge issues an order allowing them to interfere with a person's private life.²⁸

It should be noted specifically that beyond the access described just now, which is controlled by a judge, the Federal Security Service²⁹ and the internal affairs agencies³⁰ enjoy privileged access. Communication providers are obliged to provide technical access to both metadata and content data (i.e. databases with user subscriber information, their payments for connections and connections themselves – text and voice messages and so on) to these LEAs without the necessity of a court order. This privileged access was challenged several times in the Supreme Court of the Russian Federation, but the Court stated each time that this access is lawful and valid as it does not mean that control of government bodies is total and unlimited because of standards and norms regulating the access.³¹ A court order is still a general legal requirement, even though sometimes it can be obtained a posteriori. However, in practice it cannot be obtained at all if there is no need to use thus-acquired information as evidence.

The data subject has two general options to ensure the protection of his or her rights during data retention: administrative and judicial. The administrative procedure requires applying to the Roskomnadzor, whereas judicial redress takes the form of a civil proceeding. The data subject may require not only that violations stop but also that damages and moral harm are compensated.³² Liability of data processors may be not only civil but also administrative and criminal if the violation constitutes an offence set up by either the Code of Administrative Offences or the Criminal Code, respectively (Table 18.2).

When data processors are government bodies, their actions may also be challenged in administrative proceedings, which is different from the administrative offence regulation. The Code of Administrative Procedure describes rules of justice connected with acts and actions of government bodies, whereas the Code of Administrative Offences lies in the sphere of violations of public rules and relations between public officers and citizens/organisations. When violations take place during criminal proceedings, the data subject can apply for judicial redress in a form established by the Code of Criminal Procedure.

²⁷ Consent of the data subject is not necessary in such areas as the sphere of justice, execution of judgment, execution of government bodies' powers connected with public services and so on. Provisions on that are formulated in a broad way.

²⁸ The kinds of data that require a judicial order are described in Section 18.2 (in regard to content and non-content data).

²⁹ Decree of the President of the Russian Federation, 'Voprosy Federal'noj Sluzhby Bezopasnosti Rossijskoj Federatsii' (Decree on Federal Security Service), 11 August 2003, No. 960, sets out that the Federal Security Service has authority in the field of security.

³⁰ The basis for these obligations is Article 64 of the Federal Law on Communications, Russian Government Resolution No. 538 alongside delegated legislation adopted by federal executive bodies. Acts were examined in *Roman Zakharov v. Russia*, Appl. No. 47143/06, 4 December 2015, paras. 132–133, 196, 269 *et seq.*

³¹ Verkhovnyj Sud Rossijskoj Federatsii (Supreme Court of the Russian Federation), 5 March 2019, No. APL19-53. See also Section 18.3.3.

³² Compensation of moral harm is not effective in the Russian system as it is usually no more than a few thousand rubles.

TABLE 18.2 *Types of liability for violations of data subjects' rights*

Civil liability (based on provisions in the Civil Code and the law on personal data*)	Administrative liability (described in the Code of Administrative Offences**)	Criminal liability (described in the Criminal Code***)
Art. 24 of the Law on Personal Data names compensation of damages and moral harm as liability for breaking the law on personal data.	Art. 13.11 – violation of data protection legislation Art. 13.12 – violation of rules regulating protected information Art. 13.13 – illegal activity in the sphere of data protection Art. 13.14 – disclosure of data to which access is limited The punishments provided are mainly fines, different for persons and legal persons, from 500 rubles to 18 million rubles for different offences (around €5 to €180,000)	Art. 137 – violation of the right to respect for one's private life Art. 138 – violation of privacy of correspondence, phone conversation, post, telegraph and other messages Art. 272 – illegal access to computer information
Provisions on damages and moral harm as measures of civil liability are described in Articles 12, 15 and 151 of the Civil Code.		

Notes: * See Grazhdanskij kodeks Rossijskoj Federatsii (Russian Civil Code), 30 November 1994, No. 51-FZ. Some scholars criticise the lack of specific provisions on data protection in the Civil Code. See, e.g., V. D. Ruzanova, 'Pravo na zaschitu personal'nyh dannyh: grazhdansko-pravovoj aspekt' (2019) 6 *Grazhdanskoye pravo* 17–20.

** Kodeks Rossijskoj Federatsii ob administrativnykh pravonarusheniyakh (Russian Code of Administrative Offences), 30 December 2011, No. 195-FZ.

*** Ugolovnyj kodeks Rossijskoj Federatsii (Russian Criminal Code), 13 June 1996, No. 63-FZ.

18.2 TERMINOLOGY AND CATEGORIES

18.2.1 Data

The term 'data' does not exist in Russian criminal procedure law. The Code of Criminal Procedure uses terms that are close to the term 'data', such as 'information', 'pieces of information', but they are not specified.³³ The definition of 'personal data' can be found in Article 3 of the Federal Law on Personal Data where it is stated that personal data is information that is connected with the person identified directly or indirectly. Because of such a broad definition, much (if not all) information can be referred to as personal data. The absence of the term 'data' from laws is counterbalanced by a number of definitions which are used in different regulations and accepted by federal executive bodies and LEAs.³⁴

Such regulations in English can be called 'State Standards'. State Standards were originally developed by the government of the Soviet Union as part of its national standardisation strategy.

³³ See Ugolovno-protsessual'nyj kodeks Rossijskoj Federatsii (Russian Code of Criminal Procedure), 18 December 2001, No. 174-FZ, Arts. 13, 19, 74. In Russian there are a number of terms close to 'data' that are used by the Russian legislator. The closest term is 'dannyye', but there are also 'informatsiya' ('information') and 'svedeniya' ('pieces of information').

³⁴ Executive power is exercised by the Government of the Russian Federation. The government consists of the Chairman of the Government of the Russian Federation, deputy chairmen and federal ministers. The system of federal executive bodies is headed by the government and includes ministries, federal services and federal agencies. However, there are ministries, federal agencies and services that report directly to the President, for example the Ministry of Internal Affairs, the Ministry of Emergency Situations, the Ministry of Foreign Affairs, the Ministry of Defence and so on.

All products had to meet the requirements specified in State Standards (also well known as GOST, which is an acronym for *gosudarstvennyy standart*, meaning *state standard*). Currently, the application of State Standards by producers is voluntary, except if mandated by federal laws.

A few of them are related to the sphere of data and data protection. For instance, State Standard R 50922–2006 ‘Protection of information: Key terms and definitions’ provides for the definition of data: ‘facts, terms or commands which are formalised and which can be transferred and processed in a manual way or automatically’. State Standard 15971–90 ‘Information processing systems: Terms and definitions’ defines ‘data’ as ‘information in a form that allows for it to be processed automatically with the possible participation of a human’. State Standard R 52292–2004 ‘Information technology: Electronic information exchange – Terms and definitions’ sees ‘data’ as ‘a formalised way of presenting information that allows for communication, interpretation and the processing of information’. These State Standards are accepted by the Federal Agency of Technical Regulating and Metrology and establish the basic terms with the corresponding definitions that are used in standardisation work in some specific fields (information security, electronic information exchange and so on). They are not directly related to the criminal process, including the question of gathering digital evidence. But definitions of the basic terms contained in these Standards help in understanding how certain terms can be interpreted, in particular by LEAs and courts.

In spite of Federal Law No. 149-FZ not distinguishing between ‘data’ and ‘information’, it seems to us that State Standards define the practice in this sphere, regardless of their non-binding nature. The key idea is that data means not just information itself but different ways of working with it. This was illustrated in a case heard by the Orenburg Regional Court.³⁵ The facts of the case were as follows: A prosecutor requested information directly from a drug rehabilitation clinic on people who had applied to become its patients. The doctors refused to provide this information. Several aspects were analysed by the court. One important aspect was connected with the special regime for data connected with medical confidentiality. In asking about data and information, the prosecutor was requesting information that had been systematised so it was actually a request for data. At the same time, the drug rehabilitation centre was not able to provide it as it did not have the status of ‘personal data processor’ and, according to data protection law, it could not process information in a way that could have provided the prosecutor with the pieces of necessary information. Because of this, representatives of the clinic were not punished for their refusal; they did not have the right to process information and turn pieces of information into data.

This example shows that without the status that is connected with obligations in the sphere of data protection, a person (natural or legal) cannot be held liable for refusals to provide data to LEAs. However, these situations are not common and as a rule the one whom the request is sent to is obliged to store data and provide it to the LEAs. Operations with personal data usually require registration as a personal data processor and the example above can be explained only taking into account the fact that the centre insisted that there were no operations using personal data at all and that it did not belong to any database it would manage.

The present legislation does not make a clear distinction between different types of data. There are no exact classifications, but it is possible to distinguish between *content data* and *non-content data*. However, this distinction is not mentioned in any act and can be drawn mostly from the various ways of getting access to different types of data. Thus, it is not the nature of the data but the mechanism to get access to it which is taken into account for the classification. For

³⁵ Orenburgskij oblastnoj sud (Orenburg Regional Court), 27 February 2018, No. 33-1447/2018.

instance, Article 13 of the Code of Criminal Procedure of the Russian Federation prescribes that the restriction of the citizen's right to privacy of correspondence, telephone and other means of communication (we could say content data) is admissible only with a court decision. Intercepting postal and telegraph messages at post offices, monitoring and recording telephone calls and other conversations may be carried out only subject to a court decision,³⁶ whereas many other kinds of data (we could say non-content data) can be obtained without any court order.

Sometimes the distinction is less clear when we speak about the right to respect for one's private life. Bank secrecy covers many types of information that can be made accessible in different ways. Access to some of them requires a judicial order. For example, in some cases during operative-search activity there are pieces of data that LEAs may request only with a judicial order.³⁷ Others include many other pieces of data that are transferred to the Federal Financial Monitoring Service of the Russian Federation (the Rosfinmonitoring) without such order. While that data may be necessary to investigate criminal activity, it is also protected by bank secrecy. Nevertheless, the banks that have found out suspicious operations of a certain kind send information to other banks and to the Rosfinmonitoring without any judicial order.³⁸

18.2.2 Service Providers

National criminal procedure does not use any special terms to refer to service providers requested or required to assist LEAs in the context of criminal investigations, but refers to persons obliged by certain duties. Hence, the terms provided in other branches of law are used. The legislation on telecommunications uses the term 'operator of telecommunication', which is a legal entity or individual entrepreneur providing communication services on the basis of an appropriate licence.³⁹ As for the internet, courts in their judgments use the terms 'providers' and 'internet-providers'.

The important classification for criminal procedure purposes is the one which is based in data protection law. Firstly, there are personal data processors, which is a broad group that processes personal data in any form, including digital. These processors usually request the consent of the data subjects to process their data. All websites that collect and process their users' data fall into that category. Among them are shops that sell goods online and medical centres that work with clients' records using the internet. Secondly, within this group there are information dissemination managers that not only process data but provide communication between users via the internet. It seems they are named separately not only because of their specific nature but because of their obligations connected with data retention. Information dissemination managers include companies such as

³⁶ Russian Code of Criminal Procedure, Art. 13.

³⁷ Article 26 of the Federal Law No. 395-FZ of 2 December 1990 'On Banks and Bank Activities' (Federal'nyj zakon 'O bankakh i bankovskoj deyatel'nosti') contains a long description of different types of data protected by bank secrecy (the article itself is entitled 'Bank Secrecy'). Operative-search activities in Russia are connected with criminal procedure, but they do not fall within its boundaries. This article particularly names operative-search measures that are taken before the criminal case is opened when authorities are just trying to find out whether there are grounds to start the criminal investigation or not. Some operative-search measures may also take place while working on a criminal case, but those are not mentioned in the paragraph of the article described above.

³⁸ This mechanism is based on the purposes and provisions of the Federal Law No. 115-FZ of 7 August 2001 'On Counteracting Legalisation of Money-Laundering and Financing of Terrorism' (Federal'nyj zakon 'O protivodejstvii legalizatsii (otmyvaniyu) dokhodov, poluchennykh prestupnym putem, i finansirovaniyu terrorizma'). Many provisions are laid down by the Central Bank of the Russian Federation, for example Regulation of the Central Bank No. 5861-U of 15 July 2021 is devoted to the mechanism of transferring to the Rosfinmonitoring data mentioned in the law named above.

³⁹ Federal Law on Communications, Art. 2.

Facebook, VKontakte, WhatsApp, Viber and all the others that allow the exchange of messages.⁴⁰ As a rule, information dissemination managers often cooperate with LEAs and inform their users about it already in their terms and conditions and on their webpages.

An entity can belong to one or more categories, for example be an operator and a data processor, which also means that they are subject to different regulatory frameworks. When the duties of an entity concern communication, an organisation is subject to duties as an operator, while in other cases its status as ‘data processor’ or ‘information dissemination manager’ will define other obligations. Usually, LEAs require *personal data*, so the status of a company which is subject to data protection regulation plays a more important role than the status which is grounded in communications law.

While telecommunications operators must get a licence, information dissemination managers are not subject to this requirement. It is enough that they send a notification to the Roskomnadzor that they have started their activity. Furthermore, they are subject to different obligations (such as the above-described data retention duties), the violation of which may result in suspension of their activities.

18.3 DOMESTIC COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

18.3.1 *Introduction*

In Russia, cooperation between LEAs and service providers takes place in the framework of two kinds of activity: criminal investigation and operative-search activities. All persons (both legal and natural) that process data are obliged to cooperate with LEAs (Section 18.3.2.1). There are some instances of voluntary cooperation, but very limited (Section 18.3.2.2). One has to take into account the difference between national and transnational situations, and voluntary cooperation has some role to play in international situations. In any case, cooperation at the national level takes place in all cases when data processors are obliged to localise data on the territory of Russia. Most providers fall into this category of processors.⁴¹ Cooperation takes place in a context of a deficient human rights framework, which does not guarantee safeguarding of the rights of persons concerned by handing over of data by providers to law enforcement (Section 18.3.3).

18.3.2 *Nature of the Cooperation*

18.3.2.1 *Mandatory Cooperation*

The legal basis for mandatory cooperation can be found in different acts – not only in the Code of Criminal Procedure of the Russian Federation but also in acts regarding operative measures or regulating certain law enforcement bodies (e.g. the Federal Law on Operative-Search Activity, 12 August 2005, No. 144-FZ and the federal laws on police and the Federal Security Service). All of them provide for mandatory cooperation giving representatives of law enforcement bodies a right to apply to operators/data processors with a request to provide requested data. These laws do not contain specific provisions as regards data, but the legal basis for requests are

⁴⁰ This does not mean that providing an exchange of messages between users is their primary function and goal. For instance, the site Ficbook, which is aimed at giving people the opportunity to share their creative writing with others (non-professional writers and poets) is still an information dissemination manager as there is an ability to write messages to users and to receive them.

⁴¹ For further information, see Section 18.4.1.

provisions on requests for information from persons who might have it (authorities, organisations, companies, officials and natural persons). For example, the police are entitled 'to require and gratuitously receive upon a reasoned request of a duly authorised police officer data, certificates, documents (their copies), any other information, including personal data, from a state and municipal authority, public association, entity, official and person'.⁴² Another example can be found in the Code of Criminal Procedure of the Russian Federation: upon receipt of information on a crime, LEAs shall be entitled to require documents and objects.⁴³

The rights of LEAs to request data are mirrored by provisions obliging authorities, organisations, companies and individuals to provide LEAs with the requested pieces of data. For instance, according to the Federal Law on Communications, 'telecommunications operators are obliged to provide the authorised state bodies engaged in operative-search activities or ensuring the security of the Russian Federation . . . with information necessary to fulfil the tasks assigned to these bodies, in cases established by federal laws'.⁴⁴ The similar obligation for the information dissemination manager is listed in the Federal Law on Information, Information Technologies and the Protection of Information.⁴⁵ The duties of entities such as telecommunications operators and data processors are also set out in Russian government resolutions.⁴⁶

Mandatory cooperation duties concern measures such as monitoring and recording telephone calls, receiving information about connections between users and/or subscribers' units, searches and seizures (investigative measures),⁴⁷ as well as exerting control over the mail and other kinds of communications, monitoring telephone calls, taking information from technical communications channels and receiving computer information (operative-search measures).⁴⁸

If a measure affects the constitutional rights to private property, inviolability of home, private life, personal and family secrets, privacy of correspondence, telephone conversations, postal, telegraph and other communications, it has to be carried out on the basis of a judicial order or in exceptional cases with subsequent verification of the legality of the action by a court. Thus, the following of the above measures can be carried out only with a judicial order: monitoring and recording telephone calls, receiving information about connections between users and/or subscribers' units, exerting control over the mail and other kinds of communications, taking information from technical communications channels and other measures related to the restriction of the above constitutional rights.

In courts, data obtained through mandatory cooperation can be used as evidence, but rules differ between investigative and operative-search measures. The former are aimed at gathering evidence and their results become evidence as a rule (provided that they comply with the

⁴² Federal'nyj zakon 'O politsii' (Federal Law on Police), 7 February 2011, No. 3-FZ, Art. 13.

⁴³ Russian Code of Criminal Procedure, Art. 144.

⁴⁴ Federal Law on Communications, Art. 64.

⁴⁵ Federal Law on Information, Information Technologies and the Protection of Information, Art. 10.1.

⁴⁶ A government resolution is a normative act (regulatory enactment) adopted by the Government of the Russian Federation within the limits of its competence and of binding effect on the whole territory of Russia. For example, Russian Government, 'Ob utverzhdenii Pravil vzaimodejstviya organizatorov rasprostraneniya informatsii v informatsionno-telekommunikatsionnoj seti "Internet" s upolnomochennymi gosudarstvennymi organami, osushchestvlyayuschimi operativno-razysknuyu deyatel'nost' ili obespechenie bezopasnosti Rossijskoj Federatsii' (Resolution on Approval of Regulations of Interaction of Information Dissemination Managers with Authorised State Bodies Engaged in Operational Investigative Activities), 31 July 2014, No. 743, obliges information dissemination managers to provide access to their information systems to the Federal Security Service.

⁴⁷ Russian Code of Criminal Procedure, Arts. 186, 186.1, 182, 183.

⁴⁸ Federal'nyj zakon, 'Ob operativno-razysknoj deyatel'nosti' (Federal Law on Operative-Search Activity), 12 August 2005, No. 144-FZ, Art. 6.

requirements for evidence, which means that they are relevant, reliable and admissible).⁴⁹ Operative measures are not directly connected with evidence and their results, as a rule, are not pieces of evidence. Data subjects have fewer guarantees during operative-search activity than during investigative measures (which is due mainly to their secrecy), so the provision on evidence is aimed at protection of their rights. However, there is a way of turning the result of an operative-search activity into a piece of evidence, which is done through so-called processualisation. If there is an alternative investigative measure to the operative-search one, then this investigative measure should be carried out to create admissible evidence. However, if there is none and/or if the operative-search measure cannot be repeated with the same effect, then the results of this measure are included by means of interrogation of the authority that undertook the operative-search measure, usually an operative officer, who describes the measure and its results.

The admissibility of evidence can be challenged by parties to the criminal proceeding, or the court may declare a piece of evidence inadmissible on its own initiative. Representatives of third parties who do not belong to the prosecution or defence can challenge actions that interfere with their rights, but not the admissibility as such. For example, an entity whose databases and equipment have been seized can challenge in court actions that affect their rights.

Cases in which data processors/operators may try to challenge requests of LEAs in court are usually connected with situations when the necessity of judicial orders to get certain kinds of data is not obvious and clear. The following example will provide illustrations of the Russian approach in that respect.

The example concerns Telegram, a popular messenger service. The Russian law provides for rules according to which a service provider may be forced to change the technical infrastructure or security settings of its services in order to make them interceptable. Part 4.1 of Article 10.1 of the Federal Law on Information, Information Technologies and the Protection of Information states that if information dissemination managers use a special code system while receiving, transmitting, delivering and/or processing electronic messages, they are obliged to provide the Federal Security Service with the encryption key which is needed to decode the received, sent, delivered and/or processed emails. This norm was adopted in 2016 and justified as a counterterrorism measure.⁵⁰ The procedure is partly regulated by the Federal Security Service itself.⁵¹

Telegram declined to provide the encryption code for some messages, citing lack of technical capability. The court ruled that according to the law Telegram is obliged to make it technically possible for the federal body to decrypt the messages if needed.⁵² Because of non-compliance,

⁴⁹ In our system, these requirements are interpreted as follows: relevance means that pieces of evidence refer to issues of the case, so that irrelevant information is not just used to influence judges or the jury; reliability means that pieces of evidence obtained are faithful and correspond to real facts; admissibility as a requirement includes several aspects and means that pieces of evidence can be obtained only by an appropriate authority that takes an appropriate investigative measure and it does this legally. See, e.g., Golovko, *Kurs ugovnogo protsesssa*, 446–455; V. V. Zolotykh, *Proverka dopustimosti dokazatel'stv v ugovnom protsesse* (Rostov-na-Donu: Feniks, 1999); N. M. Kipnis, *Dopustimost' dokazatel'stv v ugovnom sudoproizvodstve* (Moscow: Urist, 1995); T. P. Ishmayeva, 'K voprosu o juridicheskikh svoistvah dokazatel'stv v ugovnom protsesse' (2015) 23(44) *Vestnik Chelyabinskogo gosudarstvennogo universiteta* 133–136.

⁵⁰ Explanatory Note to Bill No. 1039149-6.

⁵¹ 'Ob utverzhdenii Poryadka predstavleniya organizatorami rasprostraneniya informatsii v informatsionno-telekommunikatsionnoj seti "Internet" v Federal'nyu sluzhbu bezopasnosti Rossijskoj Federatsii informatsii, neobkhodimoy dlya dekodirovaniya primimayemykh, peredavaemykh, dostavlyayemykh i (ili) obrabatyvaemykh elektronnykh soobshchenij pol'zovatelej informatsionno-telekommunikatsionnoj seti "Internet"' (Act of the Federal Security Service), 19 July 2016, No. 432, Arts. 2–6.

⁵² Moskovskij gorodskoj sud (Moscow City Court), 14 June 2018, No. 33-24870/2018; Russian Supreme Court, 9 August 2018, No. APL18-298.

Telegram was blocked in Russia. This measure was seen by some scholars as too intrusive and at the same time useless because the majority of users managed to overcome the blockade.⁵³ In addition, despite the blockade, Telegram was extensively used by the Russian governmental bodies to deal with the coronavirus pandemic, for example by providing instructions to citizens stuck abroad on how to return to Russia.⁵⁴ That is why, in June 2020, a bill was introduced in the State Duma with the provisions which would allow Telegram (and some other blocked messengers) to operate legally.⁵⁵ The bill was rejected in 2021, but in 2020 the CEO of Telegram, Pavel Durov, already agreed to cooperate with LEAs and the Roskomnadzor eliminated all restrictions.⁵⁶

Further, courts dealing with refusals of telecommunications operators to provide requested data put emphasis on secrecy of communications, instead of the right to privacy in general. Judges also show inconsistencies in their approach to accessing data. For instance, the Supreme Court of the Russian Federation stated that a judicial order is not necessary to get the IP address of a static or dynamic user, as requests concerned only the user's data and not his/her communications.⁵⁷ As for international mobile equipment identity (IMEI) requests, the position of the courts depends on the circumstances of a case. In one case the refusal of a telecommunications operator to provide data on IMEI codes and users' identification without a judicial order was considered lawful by the Supreme Court.⁵⁸ The Court stated in that case that the LEA required data that included data on connections between users among other things and therefore it needed a judicial order for the required data. In another case an investigator required information about the owner of a phone with a particular IMEI code – his subscriber identity module (SIM) card number, the passport data of the subscriber to whom the SIM card was registered and whether there were any phone calls within a particular period of time. The Court qualified it as a request connected only with the personal data of the user. A judicial order was considered to be unnecessary.⁵⁹ As the Court noted, the investigator had information about the IMEI; therefore, there was no need to identify the subscriber device.⁶⁰

On 1 June 2017, the Plenum of the Supreme Court of the Russian Federation indicated:

A judge may give permission to receive information about the date, time, duration of connections between subscribers and[/or] subscriber devices (user equipment), subscriber numbers, other data that can identify subscribers, as well as information about the numbers and location of

⁵³ D. V. Abdrahmanov, 'Blokirovka Telegram v Rossii: konstitutsionno-pravovoj aspekt' (2018) 7 *Constitutsionnoye i munitsipal'noye pravo* 35–38.

⁵⁴ See, e.g., Ministerstvo inostrannykh del (Ministry of Foreign Affairs), Official Telegram page, https://telegram.me/MID_Russia (accessed 18 March 2023).

⁵⁵ Zakonoproekt 972279-7 'O vnesenii izmenenij v Federal'nyj zakon "Ob informatsii, informatsionnykh tekhnologiyakh i o zaschite informatsii"' (Bill No. 972279-7 'On Amendments to the Federal Law on Information, Information Technologies and the Protection of Information'), 15 June 2020, <https://sozd.duma.gov.ru/bill/972279-7>.

⁵⁶ Telegraphnoye Agentstvo Sovetskogo Soyuza (TASS or Russian News Agency), 'Roskomnadzor razblokiruet Telegram', 18 June 2020, <https://tass.ru/obschestvo/8759695>; TASS, 'Istoriya blokirovki Telegram v Rossii', 18 June 2020, <https://tass.ru/info/8761201>.

⁵⁷ Verkhovnyj Sud Rossijskoj Federatsii (Russian Supreme Court), Postanovleniye (Resolution), 30 March 2016, No. 82-AD16-1, paras. 25–30. (A resolution is a form of an act of court (or **judicial act**) along with sentences, decisions, rulings, orders. The form of a judicial act depends on the type of legal proceedings (criminal, civil, administrative), the stage of legal proceedings (e.g. proceedings in the court of the first instance or **appeal proceedings**), as well as the issue resolved in a judicial act. Any court act that has come into legal force is subject to execution on the whole territory of the Russian Federation.)

⁵⁸ Verkhovnyj Sud Rossijskoj Federatsii (Russian Supreme Court), Postanovleniye (Resolution), 11 October 2016, No. 82-AD16-5, paras. 14–17.

⁵⁹ Kirovskij rayonnyj sud goroda Irkutsk (Kirovskij Court of Irkutsk), 18 April 2016, No. 2-1591/2016, paras. 35–36.

⁶⁰ Kirovskij Court of Irkutsk, paras. 47–48.

transceiver base stations. Other data that allows identification of subscribers may include, in particular, information about the IMEI code of the subscriber unit or the location of the telephone set relative to the base station.⁶¹

Refusal to cooperate in the Russian legislation means that operators/data processors do not fulfil their legal obligations or fulfil them in an incorrect way and incur liability. In practice it may include refusal to provide data, not providing data on time or providing it in an insufficient way. As for the time to reply for operators/data processors, if a provider is unable to fulfil the request within the given deadline, it must inform the authority that issued the request about the period of time in which it is able to provide the required information and explain the reasons why it is unable to provide the information in due time. If operators/data processors follow this procedure, they are not liable for a late or slow reply.⁶² If data processors do not possess the required information, they can be liable only if they are obliged under the law to store it but do not do it.

The refusal to cooperate may also consist in refusing to provide remote access to databases and information systems for the Federal Security Service or to provide information necessary to decode or decrypt messages. In such cases, access to the information systems and/or programs which are provided by this service provider will be restricted by the court decision in an administrative proceeding in accordance with Art. 15.4 of the Federal Law on Information, Information Technologies and the Protection of Information until such duties are fulfilled.

Finally, it may also include the refusal to establish equipment allowing LEAs to get access to information necessary for reasons related to the security of the country. Duties related to these issues are provided by federal laws and/or licence agreements. In case of a refusal to cooperate, operators and data processors are liable according to the Code of Administrative Offences of the Russian Federation. The liability can be imposed by either specified bodies (mostly the Roskomnadzor) or the court. In most cases, the sanctions are fines (different for natural persons and legal persons).⁶³ The Code of Administrative Offences establishes which action (omission) of a natural person or legal person is an administrative offence and is punishable by imposing an administrative penalty (which can be regarded as punitive in the European Convention on Human Rights (ECHR) sense),⁶⁴ although the fine is not significant.

More important fines may be imposed for *failure to perform a duty* to store and/or provide information on the facts of reception, transmission, delivery and/or processing of voice information, written text, images, sounds or other electronic messages of internet users and information about such users. This failure may lead to an administrative fine of 800,000 rubles to 1,000,000 rubles (approximately €10,000) for legal persons; of 30,000 rubles to 50,000 rubles

⁶¹ Russian Supreme Court (Plenum), 'O praktike rassmotreniya sudami khodatajstv o proizvodstve sledstvennykh deystviy, svyazannykh s ogranicheniyem konstitutsionnykh prav grazhdan (stat'ya 165 UPK RF)' (Resolution on the Practice of Consideration by Courts of Applications for Investigative Actions Related to the Restriction of Constitutional Rights of Citizens (Article 165 of the Code of Criminal Procedure)), 1 June 2017, No. 19, para. 11. On plenary sessions the Supreme Court studies judicial decisions of lower courts on various topics and adopts resolutions, which establish recommendations on the interpretation of particular provisions of law for lower courts to ensure uniform application. Plenary sessions must be attended by all judges of the Supreme Court. The plenum of the Supreme Court is not any judicial instance; it does not consider the merits of the case. Its resolutions are not decisions that concern any specific case. Legally, resolutions of the Supreme Court Plenum are not binding on the lower courts; however, in fact, all courts follow them because otherwise the court decision can be reversed by a higher court.

⁶² Resolution on Information Storage Regulations by Information Dissemination Managers, para. 11.

⁶³ Russian Code of Administrative Offences, Arts. 17.7 and 19.7.

⁶⁴ See, e.g., *Sergey Zolotukhin v. Russia*, Appl. No. 14939/03, 10 February 2009; *Nemtsov v. Russia*, Appl. No. 1774/11, 31 July 2014; *Mikhaylova v. Russia*, Appl. No. 46998/08, 19 November 2015; and so on.

(approximately €500) for officials; and of 3,000 rubles to 5,000 rubles (approximately €50) for natural persons.⁶⁵ The same penalties may be imposed for failure by an information dissemination manager to provide the federal executive body responsible for security with the necessary information required to decode the received, transmitted, delivered and/or processed electronic message.⁶⁶

Special sanctions are mentioned by federal legislation on information. They include blocking of the service offered by data processors and limiting their access to information programs and systems that are designed and/or used to receive, transmit, deliver and/or process electronic messages from internet users.⁶⁷ In practice the most important sanction is blocking access to websites: in this case the network addresses (IP addresses and/or domain names) of such internet services are included in a special Register maintained by the Roskomnadzor. This provision is perhaps the strongest incentive for companies to comply with the law. This special sanction may be imposed alongside the fine assigned for the commission of an administrative offence.

Operators/data processors can ask for additional information only if the request does not contain all the information that is necessary to fulfil it. They cannot make any cooperation conditional. Operators/data processors can only justify the refusal to cooperate on the basis of the legal requirements for the request. It is assumed that all complex and controversial issues such as conflicting legal obligations have already been solved by the law.⁶⁸ Legal requirements for the request that usually become defences for data processors/operators are primarily from three groups of requirements:

- those connected with the authority who must be empowered to issue such a request;
- those connected with the grounds for a request that must make the request valid enough;
- those connected with the judicial order that is necessary to get some types of data.

Besides the question of judicial order, which we discussed earlier, other requirements come into play. The general requirement imposed on all requests of LEAs is that they must be reasoned. The request must indicate the grounds for requesting information. In practice it is not always fulfilled. A court considered that a request was invalid when it did not contain information on the concrete criminal case for the purposes for which the data was requested. The mere fact that the LEA stated it needed that data was considered insufficient.⁶⁹ Another requirement for a request is that it has to be issued on a predesigned form. Some judgments considered refusal to cooperate to be justified when requests were sent in the form of an electronic message and not using that form.⁷⁰ However, operators/data processors often cooperate when requests are in a digital form, stating at the same time in their replies that the original of the request must be sent to them in a paper-based form. Such flexibility of service providers is explained by the fear of sanctions.

⁶⁵ Russian Code of Administrative Offences, Art. 13.31, s. 2.

⁶⁶ Ibid., Art. 13.31, s. 2.1.

⁶⁷ Federal Law on Information, Information Technologies and the Protection of Information, Art. 15.4.

⁶⁸ As we have already noted, not all issues have actually been covered by the law. The nature of certain kinds of information is not clear for courts and is not yet a matter of interest for the legislator (e.g. an IMEI request). What is more, the way the law intends to solve the problem of conflicting legal obligations is rather simple and includes only the mechanism of judicial orders to get certain data. However, in practice this solution is neither universal nor ideal.

⁶⁹ Astrakhanskij oblastnoj sud (Astrahan regional court), 16 July 2015, No. 4a-303/2015, paras. 15–17.

⁷⁰ Leninskij rajonnyj sud goroda Ul'yanovska (Leninski Court of Ulianovsk), 6 December 2017, No. 12-924/17, paras. 10–11.

18.3.2.2 Voluntary Cooperation

In the Russian national system, voluntary cooperation hardly exists and is mostly associated with foreign companies. Thus, the statistics made available by Google reflect that in 2020, from July to December, it provided data for only 17 per cent of requests from Russia, from January to June in 8 per cent of cases.⁷¹ In 2021, from January to June, some data was passed to LEAs in 8 per cent of cases, from July to December in 28 per cent (Google doesn't specify percentage in regard to types of data). Requests are examined by the service provider, in this case Google, who does it according to its own rules.⁷² There is no clear legal basis for such voluntary cooperation under Russian law, although it appears to be practised.

At the national level, voluntary cooperation is possible as an exception in situations where data processors/operators are not obliged to provide data due to deficiencies of the request (e.g. in compliance with its conditions). For instance, authorities may send a direct request while a judicial order is necessary. However, we believe that, in practice, the cooperation is not fully voluntary, as the authority may obtain the order subsequently. In our opinion, cooperation in such cases constitutes a violation of the rights of data subjects, but it seems that it is currently acceptable. Our research into practice revealed that in similar situations concerning bank secrecy, smaller banks will usually comply with requests lacking judicial warrants, while major financial institutions would still require it. Our contacts also revealed that they never had cases of refusal by a court to issue a warrant, demonstrating that this guarantee is rather fictional. While providing data without a judicial order (when one is necessary) may incur liability towards customers, in practice this threat is limited, because in many cases data subjects do not know their rights are being or have been violated.⁷³

18.3.3 Protection of Human Rights

In the Russian legal system, the attitude of the legislator towards cooperation between service providers and LEAs is controversial. On the one hand, the key priority is security, which is interpreted in a broad way. The term security in national legislation includes not only counter-terrorism security but also national, economic, military, information and ecological security. The main task of operative-search activity is to guarantee that security.⁷⁴ Moreover, the Russian legal system pays much attention to counter-extremism measures, meaning that they are also necessary to provide national security. This leads to a variety of instruments being used by law enforcement bodies that are devoted to prevention of many kinds of activities. Not all of these instruments manage to find a balance between national security and human rights. Thus, many pieces of information are kept in law enforcement programs and databases for a long time. This is well illustrated by the European Court of Human Rights (ECtHR) case of Sergey Shimovolos, who claimed that he was arrested because of information about a ticket he bought to a city where extremists were active during that period of time.⁷⁵ Information connected with Shimovolos' travel across the country was passed to the law enforcement bodies automatically, as his name

⁷¹ Google Transparency Report, 'Global Requests for User Information', <https://transparencyreport.google.com/user-data/overview>.

⁷² Google Privacy & Terms, 'How Google Handles Government Requests for User Information', <https://policies.google.com/terms/information-requests>.

⁷³ For further information, see Section 18.3.3. This lack of knowledge exists because of operative-search measures.

⁷⁴ For example, this meaning of security, as well as tasks of law enforcement bodies, is mentioned in Federal Law on Operative-Search Activity.

⁷⁵ *Shimovolos v. Russia*, Appl. No. 30194/09, 21 June 2011, paras. 6–7.

was included in the surveillance database. Interestingly, in the surveillance database he was included in the category of human rights activists, which was sufficient to consider him to be high risk to national security.

On the other hand, it must be taken into account that the Constitution of the Russian Federation states that human rights and freedoms are of great importance. Thus, there are some legal tools created to protect human rights, the most important of which is judicial review. The Constitutional Court of the Russian Federation quite often describes the essence of this institution and its important role, though in practice it should not be overestimated. For instance, the ECtHR ruled that the Russian judicial review is ineffective as many Russian courts do not thoroughly check whether it is really necessary to interfere with the exercise of someone's right to respect their private life or not.⁷⁶ They do not require any additional information. The request itself on many occasions becomes the only necessary ground to issue a judicial order.⁷⁷ There are some bodies that are also aimed at human rights protection such as the Ombudsman of the Russian Federation and regional ombudsmen.

Moreover, the reasons for the current balance of values in our national system are connected with some historical assumptions. The role of the security services has been important for many years and is sometimes mentioned by the judges of the Constitutional Court in their dissenting opinions. For example, Judge Morschakova in her dissenting opinion to the decision of the Constitutional Court called this feature 'the long-established preferences to security services' interests'.⁷⁸ This practice has resulted in relatively unhindered cooperation between LEAs and providers.

In addition, in the Russian culture the essence of privacy is sometimes misinterpreted. The so-called nothing-to-hide argument is widespread among the citizens, which means that they are not always interested in the protection of their own rights.

Furthermore, data subjects are not always informed of service providers' cooperation with LEAs. There is an important difference between criminal procedure and operational-search activities. Criminal procedure activities aim at providing evidence which is submitted to a court for trial. All criminal defendants, before the indictment is sent to the court, have a right to read and analyse the file, which is why they are informed about all pieces of foundation evidence.

On the other hand, operative-search measures, even if they are closely connected with criminal procedure, do not necessarily lead to a trial (or to opening of an official criminal procedure). Information about a certain person can be collected over several years without a criminal case being initiated. The person whose data is collected usually does not have the opportunity to be informed about it, even after the operative-search activity has stopped. The Constitutional Court of the Russian Federation as well as the Supreme Court consider secrecy to be a fundamental principle for operative-search activity, even when the measure is finished.⁷⁹ The ECtHR, however, has regarded this feature of the Russian system as questionable because of the obvious fact that lack of information leads to lack of possibilities to protect one's rights.⁸⁰

⁷⁶ *Roman Zakharov v. Russia*, para. 263. This conclusion is based on analytics prepared by the Russian courts of general jurisdiction (presented by Roman Zakharov). The ECtHR stated that materials allowed it to conclude that in their daily practice Russian courts did not check whether interference was reasonable, necessary and proportionate.

⁷⁷ This approach is supported by some authors: because of the high level of crime, it is too early to modify norms and establish protection of personal data as a key priority. See, e.g., N. I. Petrykina, *Pravovoye regulirovaniye oborota personal'nykh dannykh* (Moscow: Statut, 2011).

⁷⁸ Russian Constitutional Court, 14 July 1998, No. 86-O.

⁷⁹ For example, the position of the Constitutional Court was reflected in its decision No. 86-O and has not changed since that time. The Supreme Court supports its position in many decisions too. See Verkhovnyj Sud Rossijskoj Federatsii (Russian Supreme Court), Decision of the Appeal, 25 October 2017, No. 49-APG17-34.

⁸⁰ *Roman Zakharov v. Russia*, paras. 286–290.

Even if a person occasionally gets information on certain operative-search measures that are conducted to receive/store/process one's data, it is very difficult to protect one's rights. Information on these operative-search measures is protected by state secrecy. The Constitutional Court of the Russian Federation stated in one of its decisions that a person does not have a constitutional right to request all data collected on them if the data has been collected according to the Constitution and the law.⁸¹ The way to protect one's rights becomes connected with the mechanism of judicial control. The court evaluates whether there are grounds to interfere with the private life of a person, whether there should be a judicial order and whether that order was appropriate. The regime of state secrecy leads to the evaluation of all facts by the court itself, resulting in a non-public reasoning in these decisions, so it is not clear which facts were the basis of each decision of that kind. Moreover, there is no transparency in how long these pieces of information are protected by the regime of state secrecy and what are the procedures and conditions for transferring materials or individual documents to the open access regime.⁸²

It is worth noting that in the case of post parcels, the person to whom the parcel was addressed is informed, after the parcel was opened for security reasons and if nothing dangerous was found. The same mechanism is still not used for messages in an electronic form, though it is sensible to apply the same action to them as all these cases fall within the category of protection of the secrecy of one's private life.⁸³

Actions of LEAs that have interfered with the private life of individuals can also be challenged by the superior authority in the hierarchy or in a prosecutor's office. The key peculiarity remains the same: information is not provided to a data subject because of state secrecy. The Supreme Court has explained that personal files opened during operation-search activities and judicial orders allowing interference with private life and getting access to certain kinds of personal data can be given only to government bodies and authorities directly named by the law in certain cases. Even if guilt has not been proved, one can only get those pieces of information that do not break the principle of secrecy when they become accessible.⁸⁴

There are four key procedures allowing for judicial review and redress. They are as follows.

Firstly, data subjects who claim that their rights were violated can be suspects/defendants in a criminal case. Criminal procedure in Russia has two main stages – pre-trial investigation and a court trial. Rights can be protected at both stages due to the right to challenge actions of authorities in a court. This kind of procedure also deals with admissibility of evidence. The data subject can apply to the court asking to exclude a piece of evidence as inadmissible or the court

⁸¹ Russian Constitutional Court, No. 86-O.

⁸² This is strongly criticised by scholars. Scheglov states that there is no possibility to get any information for a data subject whose data was collected during operative-search activity. See Ye. N. Scheglov, 'Zaschita personal'nykh dannyykh grazhdan v delah operativnogo ucheta' (2017) 3 *Obschestvo i pravo* 61. Pashnev states:

No doubts that the person can 'claim'. However, he will never receive truly complete information, since it is easy to hide it behind a veil of state secrets or 'requirements of conspiracy', which are not defined at the legislative level and therefore can be interpreted broadly depending on the interests of the body carrying out operative-search activities or its individual officials.

See D. V. Pashnev, 'Ponyatiye i klassifikatsiya sledov prestupnogo ispol'zovaniya comp'yuternykh tekhnologiy' (2004) 2 *Comp'yuternaya prestupnost' i terrorism* 159–161.

⁸³ We understand that it will place even more work on those who are authorities of LEAs. Nevertheless, provisions that provide too many opportunities to misuse the office are dangerous for society, as there is a broad interpretation of grounds to interfere with private life. That is why we see that some changes are clearly necessary.

⁸⁴ Russian Supreme Court, 1 September 2010, No. 60-G10-4.

can do it on its own initiative. Another party to the criminal proceedings can challenge the admissibility of evidence too, but operators and data processors do not have such a possibility.

Secondly, damages caused by unlawful actions or failures to act of government bodies/authorities can be compensated during civil proceedings according to Article 1069 of the Civil Code of the Russian Federation. This article includes compensation for property damages and moral harm. Civil liability exists independently from other kinds of liability. It means that there can be both civil and disciplinary liability, civil and administrative liability and so on. This was highlighted by the Constitutional Court of the Russian Federation.⁸⁵

Thirdly, data subjects have a right to challenge actions or acts/failures to act of government authorities. Many matters connected with LEAs' acts take place within the boundaries of administrative procedure. For instance, the Supreme Court declared acts on equipment installed to provide remote access to databases for the Federal Security Service of the Russian Federation legal and valid and stated that they were of a technical character and did not violate any rights.⁸⁶

Finally, data subjects may apply to the Constitutional Court for the constitutional review of norms that were applied in their cases (they are not allowed to challenge the constitutionality of norms *in abstracto*). While provisions on criminal procedure and operation-search activities quite often become the object of a constitutional review, they have so far not led to a major reconceptualisation in view of technological developments.

18.4 CROSS-BORDER COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

18.4.1 Data Localisation

One of the most discussed features of the Russian legal framework of cooperation between LEAs and internet service providers is the data localisation obligation introduced by the amendment of the Federal Law on Personal Data,⁸⁷ which was adopted on 21 July 2014 and came into force on 1 September 2015.⁸⁸ The new provision envisages that data controllers, when collecting personal data of Russian citizens online or offline, are obliged to record, systematise, accumulate, store, update, change and retrieve such data in databases located within the territory of the Russian Federation, with certain exceptions.⁸⁹ This requirement is considered to be unique in its overreaching nature and has ensured additional opportunities

⁸⁵ This is reflected, for example, in the decision of the Constitutional Court No. 7-O of 16 January 2018 on Article 1069 of the Civil Code of the Russian Federation. The Court stated there is a clear distinction between civil liability and other kinds of liability so that if disciplinary sanctions are put on a violator, it does not mean that the violator cannot be at the same time responsible for damages according to civil law.

⁸⁶ This matter was analysed by the ECtHR in 2015 (*Roman Zakharov v. Russia*). See the following acts on equipment – Gosudarstvennyj komitet po svyazi i informatizatsii (Committee on Communications and Informatization), 20 April 1999, No. 70, Ministerstvo svyazi (Ministry of Communications), 25 July 2000, No. 130. The ECtHR stated that these acts can actually violate constitutional rights in spite of the statement that they are technical and not legal in nature (para. 241).

⁸⁷ Federal Law on Personal Data, Art. 18, s. 5.

⁸⁸ Federal'nyj zakon, 'O vnesenii izmenenij v otdel'nyye zakonodatel'nyye akty Rossijskoj Federatsii v chasti utochneniya porjadka obrabotki personal'nykh dannykh v informatsionno-telekommunikatsionnykh setyakh' (Federal Law on Amendments to Certain Laws of the Russian Federation Concerning Personal Data Processing in Information and Telecommunications Network), 21 July 2014, No. 242-FZ.

⁸⁹ Usage of databases on the Russian territory is not obligatory only if there are specific purposes – that is, if data processing is required for the purpose of meeting the goals of international agreements or statutes, or for the purposes of compliance with obligations imposed on the data controller by the Russian legislation; if it is performed for the

for Russian LEAs.⁹⁰ By adopting this rule, the legislators have assured that data can be fairly easily obtained by Russian LEAs without the difficulties linked with mutual legal assistance.

Provisions on data localisation apply to non-Russia entities according to the Federal Law on the Activities of Foreign Persons on the Internet on the Russian Territory, adopted in 2021. Its adoption was motivated by a large number of foreign companies which offer services to Russian citizens or process their data, but do not establish offices in Russia and fail to abide by obligations listed by the Russian law.⁹¹

Generally, foreign entities fall under the Law if they process data of Russian users and more than 500,000 Russian users access their information systems or internet sites during a 24-hour period. However, if their internet sites or computer programs provide opportunities to exchange electronic messages, there is no need to prove such a number of users per twenty-four hours (it means that such a company is an information dissemination manager).⁹² Then the criterion of ‘target’ can be applied to determine whether an entity is obliged to comply with the Russian law.⁹³

The Law on Foreign Persons refers to the data localisation obligation in the Law on Personal Data and lists a variety of sanctions for its violation. If a data processor operates on the territory of another country and does not meet the criteria of activity on the internet on the Russian territory, this obligation does not apply to it. The Roskomnadzor analysed principles of international law and came to the conclusion that non-residents are not obliged by Russian legal provisions, if they are located and operate on the territory of another state.⁹⁴

So, the data localisation obligations concern personal data gathered purposefully and directly from data subjects. Any personal data of Russian citizens collected by data operators must be stored on servers, in IT systems, databases or data centres located in Russia. Data’s link with Russian citizens is difficult to follow as it is not always possible to make a link between the user and his or her nationality. The Roskomnadzor has issued explanations that it would be the responsibility of data controllers to identify the nationality of the user or, in case of doubt, to localise all personal data on the territory of Russia in order to remain compliant.⁹⁵ Furthermore, although the data protection law does not expressly stipulate it, the data localisation requirement is interpreted as prohibiting the storage of personal data of Russian citizens outside Russia without first locating the personal data of Russian citizens in Russia.⁹⁶ Therefore, local and

purposes of law enforcement; or if it is performed by government agencies authorised in the course of provision of public services; or if it is performed by media or journalists in the course of performance of their professional activities or in the course of scientific or other creative activities, provided that the rights and the legitimate interests of the data subject not be harmed.

⁹⁰ A. Saveliev, ‘Russia’s New Personal Data Localization Regulations: A Step Forward or a Self-Imposed Sanction?’ (2016) 32 *Computer Law and Security Review* 128–145.

⁹¹ Poyasnitel’naya zapiska k zakonoproektu 1176731-7 ‘O deyatel’nosti inostrannykh lits v informatsionno-telekommunikatsionnoy seti “Internet” na territorii Rossijskoj Federatsii’ (Explanatory Note to Bill No. 1176731-7 ‘Federal Law on the Activities of Foreign Persons on the Internet on the Russian Territory’), 21 May 2021, <https://sozd.duma.gov.ru/bill/1176731-7>.

⁹² Federal Law on the Activities of Foreign Persons on the Internet on the Russian Territory, Art. 4.

⁹³ See also Section 18.1.2.

⁹⁴ Ministry of Digital Development, Communications and Mass Media, ‘Processing and Storage of Personal Data in the Russian Federation: Changes since 1 September 2015’, 12 February 2016, <https://digital.gov.ru/en/personaldata/>.

⁹⁵ Letter of explanation issued by the Vice-Head of the Roskomnadzor, A. A. Priezzheva, in relation to the application of the member of the Council of the Federation L. N. Bokova, No. 08AP-3572, 19 January 2015. See also Ministry of Digital Development, Communications and Mass Media, ‘Processing and Storage of Personal Data’. Such a view is shared by A. Saveliev, who states that ‘it is impossible to avoid discretion of data processors and use of presumptions’. See A. Saveliev, *Nauchno-prakticheskij Kommentarij k Federal’nomu zakonu “O personal’nykh dannyx”*, 2nd ed. (Moscow: Statut, 2021), 335–345.

⁹⁶ See also Ministry of Digital Development, Communications and Mass Media, ‘Processing and Storage of Personal Data’, 12 February 2016.

foreign companies that are data operators must process or organise the processing of personal data of Russian citizens in Russia in the first place, subject to compliance with all other general requirements of the data protection legislation.

Violation of the requirements on data localisation is punished with administrative fines according to subsection 8 of Article 13.11 of the Code of Administrative Offences:

- for natural persons: 30,000–50,000 rubles (approx. €400–€660)
- for public officials: 100,000–200,000 rubles (approx. €1,300–€2,600)
- for legal persons: 1 million–6 million rubles (approx. €13,300–€80,000).

For a repeat offence the fines are two to four times higher. In 2021 WhatsApp was fined for the first time, and Twitter and Facebook were fined for a repeat offence (i.e. their failure to localise data of Russian users).⁹⁷

Other measures include powers to block access to websites and other limits. Information sources (in particular, internet sites or computer programs) of information dissemination managers can be blocked in accordance with judicial decisions, as well as sources of violators of personal data legislation.⁹⁸ For instance, LinkedIn was added to the Register of the latter for collecting information about users who were Russian citizens, its use and transmission, which were carried out without the use of databases located in the territory of Russia.⁹⁹ On appeal, the Court of Appeal also rejected the defendant's argument that a rule found in Russian legislation is not applicable to a foreign company. According to the court, activities on the internet, by virtue of their transborder, decentralised and virtual nature, do not clearly identify the geographical boundaries of such activities. Therefore, it is possible to apply special rules to these kinds of activities, even to a foreign company. The focus of LinkedIn on the territory of Russia can be proved by the Russian-language version of the website and the use of advertising in Russian, which indicates the inclusion of a Russian audience in the business strategy of the owner of the website. At the time of writing this chapter, LinkedIn is still in the Register of prohibited websites of the Roskomnadzor.¹⁰⁰

The Federal Law on the Activities of Foreign Persons on the Internet on the Russian Territory lists specific measures which can be applied to make foreign persons comply with legal obligations on data localisation (they are called 'measures of compulsion'). These provisions are in force alongside sanctions and punishments, mentioned earlier. In particular, the Roskomnadzor is empowered to restrict advertisements, transactions, transborder transfers of data, access to information systems and internet sites, and no judicial decision is required for that.

18.4.2 Transborder Transfer

To comply with the rules of localisation of data, the primary and secondary databases approach was introduced by the Roskomnadzor.¹⁰¹ The primary database is to be located in Russia and this is the database where personal data should be initially stored. Then the information can be

⁹⁷ Roskomnadzor, 'Sud oshtrafoval Facebook, Twitter i WhatsApp na 36 mln rublej za nelokalizatsiyu baz dannykh rossijskikh pol'zovatelej na territorii RF' (Court Imposed a 36 Million Rubles Fine on Facebook, Twitter and WhatsApp for Non-compliance with Their Obligations on Data Localisation), <https://rkn.gov.ru/news/rsoc/news73828.htm>.

⁹⁸ Federal Law on Information, Information Technologies and the Protection of Information, Arts. 15.4 and 15.5.

⁹⁹ Taganskij rayonnyj sud goroda Moskvy (Taganskij court of Moscow), 10 November 2016, No. 02-3491/2016, M-3709/2016.

¹⁰⁰ Roskomnadzor, 'Universal'nyj servis proverki ogranicheniya dostupa k sajtam i (ili) stranitsam sajtov seti "Internet" (Universal Services on Check Whether Access to the Website / Website Pages Is Limited), <https://blocklist.rkn.gov.ru/#anchor> (www.linkedin.com).

¹⁰¹ Saveliev, 'Russia's New Personal Data Localization Regulations', 133.

transferred to the secondary database, outside Russia, subject to the provisions of the Law on Personal Data.

Data can be transferred to other countries provided Russian law so permits. There is a difference depending whether the country is a party to the Council of Europe Convention on the Protection of Individuals with Regard to Automated Processing of Personal Data. In principle, data can be sent to those countries, although this possibility may be limited or even prohibited in order to protect the foundations of the constitutional system of the Russian Federation, morality, health, the rights and legitimate interests of citizens, or to ensure the country's defence and state security.¹⁰² In addition, the Roskomnadzor keeps a list of countries which are not party to that Convention, but ensures adequate protection of the rights of subjects of personal data.¹⁰³

Cross-border transfer of personal data to the territory of foreign states with adequate protection is still possible if one of the following conditions is fulfilled:

- (1) there is written consent of the data subject for the cross-border transfer of his/her personal data;
- (2) the possibility is provided for in international treaties to which the Russian Federation is a party;
- (3) the possibility is provided for by federal laws, and it is necessary to protect the foundations of the constitutional system of the Russian Federation, to ensure the country's defence and state security, or to ensure the security of the stable and safe operation of the transport system, and protect the interests of the individual, society and the state in the field of the transport system;
- (4) it is provided for in a contract to which the data subject is a party;¹⁰⁴
- (5) it is necessary to protect the life, health or other vital interests of the data subject or other persons in cases when it is impossible to obtain the written consent of the data subject.

In those cases the data operator must ensure that the rights and interests of the data subjects concerned are fully protected in an 'adequate manner' in the foreign country. In that context it is generally presumed that the national data protection rules apply to:

- data processing that occurs in or is targeted towards Russia;
- the collection, storage and use of personal data of Russian citizens (data subjects).

These rules are applied regardless of where the data operators are established and located. In the context of cross-border data flow, the national data protection legislation is also applicable to a certain extent if a Russian individual is a party to a data transfer or user agreement, or consents to the processing of her/his personal data by a foreign data operator.

18.4.3 *Cross-Border Cooperation*

The legal framework for the cooperation of national LEAs with foreign providers as well as of national service providers with foreign LEAs consists mostly of the mentioned federal laws, that is, the Law on Personal Data, the Law on Information, Information Technologies and the Protection

¹⁰² Federal Law on Personal Data, Art. 12.

¹⁰³ Roskomnadzor, 'Prikaz ob utverzhdenii perechnya inostrannykh gosudarstv, obespechivayuschikh adekvatnyu zaschitu prav sub'ektov personal'nykh dannykh' (Act on Approval of the List of Foreign States Providing Adequate Protection of the Rights of Personal Data Subjects), 5 August 2022, No. 128, Annex No. 2.

¹⁰⁴ This ground is not very broad, as it means that the data subject receives some profit and the data processor transfers data with the only purpose to fulfil his obligations towards the former.

of Information, the Civil and Criminal Codes and the international treaties of the Russian Federation. The provisions of the national laws were described in Sections 18.1.2 and 18.3.2.1, so this section will be dedicated only to the international instruments that are obligatory for Russia.

Russia is a party to the Council of Europe Convention No. 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 and most of the personal data legislation is based on its provisions.¹⁰⁵ Inter alia, the following exceptions were mentioned in federal law on its ratification:

- The Convention will not be applied to personal data processed by individuals exclusively for personal and family needs or classified as a state secret in the manner established by the legislation of the Russian Federation on state secrets.
- Russia reserves the right to establish restrictions on the right of the subject of personal data to access personal data about themselves in order to protect the security of the state and public order.

18.4.3.1 Council of Europe Cybercrime Convention (CC Convention)

Russia was a member of the Council of Europe until 16 March 2022. Even before its expulsion it did not participate in all the initiatives within this forum. Russia has neither signed nor ratified the Council of Europe CC Convention. In 2005 the Russian President issued an order for the Convention to be signed, but in 2008 it was repealed.¹⁰⁶

According to the national authorities, refusing to ratify the Convention is a way to protect the sovereignty of Russia. Certain provisions of the Convention (particularly Article 32 which gives a member state the opportunity to access or receive stored computer data located in other member states) are seen by Russia as a threat to its sovereignty, its national security and the rights and legitimate interests of its citizens and legal entities as they can be interpreted in a way that is inconsistent with the purposes and principles of the Convention.¹⁰⁷

18.4.3.2 Mutual Legal Assistance Treaties (MLATs)

The Russian Federation has signed many MLATs but there is a difference between provisions covering issues of mutual legal assistance and the application of these provisions. In fact, Russia has about forty MLATs that are bilateral and a number that are multilateral. Bilateral treaties were signed either by the Soviet Union (with Russia as the legal successor

¹⁰⁵ Federal'nyj zakon, 'O prekraschenii dejstviya v otnoshenii Rossijskoj Federatsii mezhdunarodnykh dogovorov Soveta Evropy' (Federal law 'On the Termination of International Treaties of the Council of Europe with Respect to the Russian Federation'), 28 February 2023, No. 43-FZ. Some agreements signed under the auspices of the Council of Europe became invalid, but the above-mentioned Convention is still not included in the list of those agreements.

¹⁰⁶ President of the Russian Federation, Rasporyazhenie 'O prekraschenii dejstviya v otnoshenii Rossijskoj Federatsii mezhdunarodnykh dogovorov Soveta Evropy' (Executive Order on Termination of International Treaties of the Council of Europe with Respect to the Russian Federation), 15 November 2005, No. 557-tp.

¹⁰⁷ The statement of the representative of the Ministry of Foreign Affairs Ilya Rogachev. He referred to the official position of the government by saying that the aforementioned provision is unacceptable and that the Russian Federation is eager to draft a new document together with members of the United Nations that prioritises national sovereignty. See TASS (Russian News Agency), 'Russian Diplomat Called the Budapest Convention on Cybercrime Obsolete', 4 December 2017, <https://tass.ru/politika/4782506>. See also TASS, 'The Ministry of Foreign Affairs of the Russian Federation Announced the Blocking of the Initiative to Combat Cybercrime', 5 December 2017, <https://tg.ru/2017/12/05/mid-rf-zaiavil-o-blokirovke-iniciativy-po-borbe-s-kiberprestupnostiu.html>.

state) or by Russia itself. For example, the Soviet Union signed MLATs with Albania, Algeria, Bulgaria, Cuba, Cyprus, Greece, Hungary, Iraq, Vietnam and Yemen. The Russian Federation itself has signed treaties with countries such as Azerbaijan, Poland, all the Baltic states, Canada, Colombia, Iran and Mongolia.¹⁰⁸ Multilateral treaties include treaties signed by either the Soviet Union or Russia as a member of international organisations such as the United Nations, the Council of Europe, the Commonwealth of Independent States and the Shanghai Cooperation Organisation.

In addition, Russia can assist other countries even when there are no provisions laid down in a treaty according to the principle of reciprocity. Cooperation of this kind can be done directly between the law enforcement bodies of Russia and a foreign state and are based on an agreement (treaty) between these bodies. An *ex ante* legal basis is necessary for a body to be allowed to enter into that kind of agreement. There are several important bodies that are involved in cooperation of that kind: the Supreme Court, the Ministry of Foreign Affairs, the Ministry of Internal Affairs, the Ministry of Justice, the Russian Investigative Committee, the Prosecutor General's Office and the Federal Security Service of the Russian Federation. The Prosecutor General's Office of the Russian Federation, for example, states that it has 104 working agreements with bodies in 78 states. Moreover, it is dealing with more than 10,000 files connected with issues of international cooperation such as extradition and detection of suspects.¹⁰⁹ The Investigative Committee of the Russian Federation has working agreements with bodies of countries such as Finland, Belarus, Kazakhstan, Germany and the United Arab Emirates.¹¹⁰

Regarding issues of international relations, it is necessary to take into consideration two issues of practical relevance. Firstly, a large number of contacts between Russian and foreign LEAs take place based on secret documents and operations. For example, the Shanghai Convention on combating terrorism, separatism and extremism and all its databases cannot be made publicly accessible because of the nature of the unlawful activities this cooperation targets. Secondly, in day-to-day operations the level of cooperation varies. Our contacts from the Investigative Committee of the Russian Federation state that all requests connected with mutual legal assistance are first passed to the prosecution service as it is responsible for international cooperation and then prosecutors send requests either to the Investigative Committee or to the Ministry of Internal Affairs. We do not have any statistical data on the quantity of requests or the level of effectiveness. When the initial requests originate from Russia, according to practitioners interviewed by us, around 50 per cent are rejected. The difficulty of receiving data was the reason for imposing data localisation. Yet, it seems to also have a positive side from the perspective of LEAs. The normal time allowed for conducting investigations in Russia is only two months, and prolonging it requires the decision of a head of the relevant investigative committee. Difficulties with international cooperation serve as perfect justification for such prolongation.

¹⁰⁸ The Prosecutor General's Office of the Russian Federation provides us with a list of these bilateral treaties on its website. See Prosecutor General's Office, 'The List of Signed Bilateral Agreements and Other Agreements on Cooperation between the Prosecutor General's Office of the Russian Federation and the Competent Authorities of Foreign States (as of November 2022)', <https://epp.genproc.gov.ru/web/gprf/activity/international-cooperation/sogl/so>.

¹⁰⁹ The Prosecutor General's Office of the Russian Federation, Official Website, 'Mezhdunarodnoye sotrudnichestvo' (International Cooperation), November 2022, <https://epp.genproc.gov.ru/web/gprf/activity/international-cooperation>.

¹¹⁰ A. I. Bastrykin, 'International Activities of the Investigative Committee of the Russian Federation', *Investigative Committee of Russia*, <https://en.sledcom.ru/international>.

As regards gathering of digital evidence, an additional problem is linked with the strict list of types of evidence in the Russian Code of Criminal Procedure. This is also reflected in the international agreements.

18.5 CONCLUSION

In Russia the main problem regarding the cooperation of LEAs with service providers is the total ambiguity about the basis on which to pursue such cooperation and the absence of a legal framework. There is no clear understanding of the differences between the types of data, and hence their legal protection. Also, because of the absence of the ‘fruit of the poisoned tree’ theory in criminal procedure, most of the data that is difficult to obtain is used/hacked in order to get the information for further investigation. For instance, data obtained by illegal access to a mobile phone by an investigator will not be accepted as evidence. However, it can lead to gathering further evidence, which would then be admissible in court.

In relation to human rights protection in the course of operative-search activity, data retention and cross-border cooperation, there are some broad notions and a wide range of obligations that cause problems and lead to the fact that security, crime prevention and human rights are not always balanced. Usually there is no problem for law enforcement bodies to get the required information, possibly because of the liability of data processors and operators for their refusal to cooperate. More and more kinds of data are available to LEAs instantly: for example, since 29 December 2022 taxi aggregators have become obliged to provide full access to their systems to the Federal Security Service.¹¹¹

Requirements concerning data localisation have become clearer than before, since the Federal Law on Activity of Foreign Persons on the Internet in Russia was adopted. However, the range of data processors targeted by the provisions on data localisation is broad and includes different categories. Violations of the Russian law may lead to administrative fines and other restrictions.

¹¹¹ Federal’nyj zakon, ‘Ob organizatsii perevozok passazhirov i bagazha legkovym taksi v Rossijskoj Federatsii, o vnesenii izmenenij v otdel’ny’e zakonodatel’nyye akty Rossijskoj Federatsii i o priznanii utrativshimi silu otdel’nykh polozhenij zakonodatel’nykh aktov Rossijskoj Federatsii’ (Federal Law on the Organisation of Passenger and Baggage Transportation by Passenger Taxi in the Russian Federation, on Amendments to Certain Legal Acts of the Russian Federation and on Invalidation of Certain Provisions of Legal Acts of the Russian Federation), 29 December 2022, No. 580-FZ, Art. 14, <http://actual.pravo.gov.ru/text.html#pnum=0001202212290039>. For more information on the bill, see also Bill No. 121564-8, 11 May 2022, <https://sozd.duma.gov.ru/bill/121564-8>.

Digital Evidence Collection in Turkey

Seçil Bilgiç^{*}

19.1 INTRODUCTION

Turkey publishes its legal acts in Turkish in the Official Gazette (*Resmî Gazete*), the daily national and official journal that publishes new legislation and other official announcements.¹ Official English translations of the majority of legislation or legal terminology, however, do not exist. Some of the existing English translations, usually available on the websites of the relevant ministries, may be confusing or subject to criticism. For instance, Turkish officials use the English term ‘rogatory’ to denote mutual legal assistance, not the ‘letter rogatory’ instrument. The applicable rules are also typically scattered around in various acts, regulations, by-laws and presidential decrees. One may be surprised to find a cybercrime definition in intellectual property or online betting legislation, or in a seemingly irrelevant omnibus bill. There is no unified source in which to find all applicable laws or treaties, which may lead judges, lawyers and scholars to easily overlook a piece of applicable legislation. For instance, some of the mutual assistance treaties that Turkey has ratified have been published in the Official Gazette, but are missing on the website of the governing body responsible for international judicial cooperation. To add more complexity, the prevalent practice in some areas may contradict both the letter and the spirit of the law. For instance, many investigative measures which are designed as last resort measures to collect evidence, such as interception of telecommunications, are often the first measures the authorities use.

Intrinsically complex due to the multiplicity of sources and linguistic problems, collection of digital evidence in criminal proceedings is still evolving in Turkey. While the existing law does not offer a definition of electronic or digital evidence,² the Court of Cassation (the highest appellate court in Turkey) defines it as ‘information and data that are stored on electronic devices or transferred through them that have value for an ongoing investigation’.³ Turkish judges, prosecutors and even regulatory bodies have great powers to collect evidence, and hence

^{*} The author wishes to thank Professor Rıfat Murat Önok for his thoughtful comments and suggestions on an earlier draft. The author also wishes to thank her husband, Yavuzhan Yılancıoğlu, for being her Aristotelian ‘other self’ in her quest for knowledge and happiness. All views herein are those of the author in her personal capacity.

¹ Resmî Gazete, www.resmigazete.gov.tr/.

² Güz Gültan, *Electronic Evidence: Privacy Concerns Relating to the Collection of Electronic Evidence: Under Turkish Legal System and Cybercrime Convention*, Master’s thesis, University of Oslo, Faculty of Law (UiO DUO) (2012), 12, www.duo.uio.no/handle/10852/39023; Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, 7th ed. (Ankara: Seçkin, 2018), 563 (arguing that there is a need for a legislative definition for electronic evidence).

³ Court of Cassation’s Assembly of Criminal Law Chambers, E. 2017/956, K. 2017/370, dated 26 September 2017; Court of Cassation’s 16th Criminal Chamber, E. 2015/4672, K. 2016/2330, dated 21 April 2016; Court of Cassation’s 16th Criminal Chamber, E. 2015/3, K. 2017/3, dated 24 April 2017. As the Court of Cassation also cites, this definition is provided by legal scholar Leyla Keser Berber – see, e.g., Leyla Keser Berber, *Adli Bilişim* (Ankara: Yetkin Yayınları, 2004), 46.

digital evidence, located in Turkey. The question often relates to minimum safeguards that national legislation must provide to prevent abuses of such power, or lack thereof. Despite such broad powers, Turkish judicial authorities may still fail to collect the relevant e-evidence as the evidence may be located abroad.

Having ratified the Convention on Cybercrime (CC Convention)⁴ only in 2014, Turkey lags behind other Council of Europe members in addressing the technological and security challenges of digital evidence gathering abroad. While cybercrime offences definitions under Turkish law are generally in line with the CC Convention,⁵ Turkey has largely not transposed the criminal procedure and international cooperation sections of the CC Convention into its domestic law.⁶ Turkish law is also silent on the procedure and safeguards related to direct contact with holders of data (such as internet service providers) by the Turkish and foreign authorities to obtain e-evidence. Hence, both the principle of *pacta sunt servanda* and the complexities of modern investigations require the reform of Turkish criminal procedure and international cooperation law with the relevance of e-evidence in mind.⁷

Against this backdrop, Section 19.2 of this chapter briefly describes the cybercrime catalogue under Turkish criminal law. Section 19.3 outlines the investigative measures⁸ that prosecutors may carry out in order to collect and secure e-evidence within the national territory, as well as discussing the voluntary cooperation of internet service providers and data localisation requirements. Section 19.4 examines the Turkish international judicial cooperation system and explains how Turkish judicial and law enforcement authorities ('police officers') obtain evidence stored in foreign jurisdictions. Section 19.5 takes the opposite approach and explains how foreign police officers may access e-evidence located in Turkey. Finally, Section 19.6 will offer some concluding remarks.

19.2 CYBERCRIMES UNDER TURKISH LAW

The Turkish penal system has a wide catalogue of cybercrimes. A uniform terminology for cybercrime, however, is lacking.⁹ Among others, scholars and courts refer to crimes that are generally committed using the means of technology and the internet as cybercrimes,¹⁰ virtual

⁴ Council of Europe, Convention on Cybercrime, ETS No. 185, 23 November 2001.

⁵ See, e.g., Alexander Seger, *Project on Cybercrime, Cybercrime Legislation – Country Profile: Turkey* (Strasbourg: Council of Europe, 4 June 2007), www.coe.int/t/dgi/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Turkey%20_4%20june%2007_En.pdf; iProceeds, *Assessment Report – Findings and Recommendations for Improvement of Guidelines and Indicators for Financial Sector Entities to Prevent and Detect Online Fraud and Money Laundering in the Online Environment: Turkey* (Strasbourg: Council of Europe, 17 August 2017), 7, rm.coe.int/3156-35-i-proceeds-assessment-report-indicators-turkey/16807be0d0. See also Servet Yetim, 'Siber Zorbalık, Türkiye ve ABD Karşılaştırması (ABD v. Drew Dosyası)' (2015) 120 *TBB Dergisi* 326–384 at 362 ('Almost all the issues in the Convention on Cybercrime are regulated as crimes in the Turkish Criminal Code.') (translated from Turkish).

⁶ For a thorough analysis of which provisions of the CC Convention have been transposed into Turkey's domestic law, see, e.g., Council of Europe, 'Country Profile: Turkey, Octopus Cybercrime Community', last updated 28 April 2020, <https://tinyurl.com/y3lc66qr>.

⁷ Dülger, 'Bilişim Suçları', 554.

⁸ Measures such as search, seizure and arrest are called 'protective measures', 'investigative measures', 'preliminary injunctions' or 'coercive measures' under Turkish law as they restrict the fundamental rights and freedoms of the subject. See, e.g., Bahri Öztürk, *Uygulamalı Ceza Muhakemesi Hukuku*, 12th ed. (Turkey: Seçkin, 2008), 537. For the purposes of this chapter, the term 'investigative measures' will be used.

⁹ See, e.g., Murat Önok, 'International Co-operation in the Fight against Cybercrimes in the Light of the Council of Europe Convention on Cybercrime' (2013) 19(2) *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* (Prof. Dr. Nur Centel'e Armağan) 1229–1269 at 1230.

¹⁰ See, e.g., Hüseyin Çeken, 'ABD'de İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğunun Hukuki Esası', Saarbrücken Hukuki İnternet Projesi, <http://archiv.jura.uni-saarland.de/turkish/HCCekeni.html>.

crimes,¹¹ internet crimes,¹² computer crimes,¹³ crimes related to computers,¹⁴ crimes committed through information systems¹⁵ or information crimes.¹⁶ Each of these definitions alludes to a different aspect of cybercrimes and, hence, excludes certain crimes with a cyber component from its scope.¹⁷ For instance, unlawful access to a computer within a closed network would not be an ‘internet crime’, which seems contrary to the purpose of coining such a term. Moreover, absence of a uniform term complicates research and analysis on applicable case law for both practitioners and the legislator.¹⁸ Given the ever-increasing number of crimes with a cyber component, for the purposes of this chapter, cybercrimes will be defined as ‘unlawful acts wherein the computer is either a tool or target or both’.¹⁹

Turkish legislature has not enacted a cybercrime-specific statute. Cybercrime definitions may be found in various statutes, including (i) the Turkish Penal Code (TPC),²⁰ (ii) the Law on Betting Activities Related to Soccer and Other Sports Matches,²¹ (iii) the Law on Debit and Credit Cards,²² (iv) the Law on Electronic Signature²³ and (v) the Law on Intellectual Property and Artistic Works.²⁴ The vast majority of cybercrimes belong to the first group.

Section 10 of the TPC, titled ‘Information Technology Crimes’, prohibits four groups of activities: unauthorised access to an information technology (IT) system (Article 243); hindrance or destruction of a computer system (Article 244); misuse of debit and credit cards (Article 245); and possession or use of prohibited devices and (computer) programs (Article 245/A). Section 9 of the TPC catalogues ‘Offences against Privacy and Confidentiality’ and governs violation of confidentiality of communication (Article 132); eavesdropping and recording of conversations between persons (Article 133); violation of privacy (Article 134); recording of personal data (Article 135); and illegally obtaining or sharing data (Article 136). Moreover, section 7 of the TPC defines and punishes the crime of obscenity; its third paragraph is akin to but broader than the crime of child pornography. There are some other provisions scattered throughout the TPC that may also be categorised as cybercrime, such as computer and communications fraud (Article 158(1)(f)) and larceny committed by use of data processing systems (Article 142(2)(e)).

¹¹ See generally Yılmaz Yazıcıoğlu, ‘Bilgisayar Ağları ile İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı’, *Uluslararası İnternet Hukuku Sempozyumu*, 21–22 May 2001, 452.

¹² See generally Feridun Yenisey, ‘İnternet Suçlarının Yeni İşleniş Biçimleri’, *Uluslararası İnternet Hukuku Sempozyumu*, 21–22 May 2001, 447.

¹³ See generally Faruk Erem, ‘Bilgisayar Suçları ve Türk Ceza Kanunu’ (1993) 69(12) *İstanbul Barosu Dergisi* 727–732 at 727.

¹⁴ See generally Hasan Dursun, ‘Bilgisayar ile İlgili Suçlar’ (1993) 24(3) *Yargıtay Dergisi* 334–339 at 334.

¹⁵ See Yener Ünver, ‘Türk Ceza Kanunu’nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi’ (2011) 59(2) *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası* 51–153 at 79.

¹⁶ See, e.g., Dülger, ‘Bilişim Suçları’, 75.

¹⁷ For a critique of each definition, see Dülger, ‘Bilişim Suçları’, 72–75.

¹⁸ Anthony Reyes, Kevin O’Shea, Jim Steele, Jon R. Hansen, Captain Benjamin R. Jean and Thomas Ralph, *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors* (Rockland, MA: Syngress, 2007), 28 (‘She also highlights the definitional issues with computer crime, computer-related crime, and cyber crime when she remarks that “a variety of definitions [for these terms] exist, and that such variations have resulted in confusion among legislators and investigators alike”.’).

¹⁹ See Mohammed Chawki, Ashraf Darwish, Mohammad Ayoub Khan and Sapna Tyagi, *Cybercrime, Digital Forensics and Jurisdiction*, Studies in Computational Intelligence vol. 593 (Cham: Springer International, 2015), 3.

²⁰ Türk Ceza Kanunu (Turkish Penal Code), Act No. 5237, *Resmî Gazete*, 12 October 2004, numbered 25611.

²¹ Futbol ve Diğer Spor Mısabakalarında Bahis ve Şans Oyunları Düzenlemesi Hakkında Kanun (Law on Betting Activities), Act No. 7258, *Resmî Gazete*, 9 May 1959, numbered 10201.

²² Banka Kartları ve Kredi Kartları Kanunu (Credit Card Law), Act No. 5464, *Resmî Gazete*, 1 March 2006, numbered 26095.

²³ Elektronik İmza Kanunu (E-signature Law), Act No. 5070, *Resmî Gazete*, 23 January 2004, numbered 25355.

²⁴ Fikir ve Sanat Eserleri Kanunu (Intellectual Property Law), Act No. 5846, *Resmî Gazete*, 13 December 1951, numbered 7981.

TABLE 19.1 *Total number of reported section 10 offences over the years*

Before 2018	2018	2019	2020	2021
7 168	2 242	7 251	6 093	8 239

Source: Adalet Bakanlığı Adli Sicil ve İstatistik Genel Müdürlüğü [Ministry of Justice, General Directorate of Criminal Records and Statistics], *Adli İstatistikler [Judicial Statistics]* (Ankara: Ministry of Justice, 2021), 49, <https://adlisicil.adalet.gov.tr/Resimler/SayfaDokuman/310520221405382021H%C4%B0ZMETE%C3%96ZELK%C4%B0TAP.pdf>.

Section 10 of the TPC was amended several times in 2016 to comply with the provisions of the CC Convention.²⁵ For instance, according to the initial version of Article 243, merely accessing a system did not constitute an offence since the *actus reus* of the crime was to ‘illegally access and remain’ in a data processing system. In line with Article 2 of the CC Convention, the current version of Article 243 punishes mere *unlawful access* by a prison sentence of up to one year or a monetary fine.²⁶

Similarly, even though the initial section 10 of the TPC lacked a provision parallel to Article 3 of the CC Convention, a later amendment bridged the gap and defined ‘illegal interception’ as a criminal offence under Article 243 of the TPC.²⁷ Likewise, the inclusion of Article 245(A) in the TPC aimed to fulfil the obligation under Article 6 of the CC Convention regarding misuse of devices.²⁸ Article 245(A) of the TPC charges the individual who ‘creates or produces a device, computer program, password or other security code for committing a crime’.²⁹

Such changes seem to precede the significant increase of reported section 10 offences. While the total number of reported section 10 offences was merely 7,168 prior to the year 2018 (Table 19.1), there seems to be a steady increase of such reported offences after 2018.

According to the official statistics by the Ministry of Justice, section 10 offences under the TPC constituted 1.4 per cent of the offences reported to prosecutors in 2021.³⁰ The same report shows that 51.4 per cent of all section 10 offences resulted in conviction, while only 19.0 per cent of such defendants were acquitted.³¹

As mentioned, the effort to ensure that the Turkish law complies with the requirements of the procedural part of the CC Convention is lagging. However, the Turkish Code of Criminal Procedure (CCP) provides specific investigative measures to collect certain categories of data from electronic devices and communications.³²

²⁵ Cahit Aliusta and Recep Benzer, ‘Avrupa Siber Suçlar Sözleşmesi ve Türkiye’nin Dahil Olma Süreci’ (2018) 4(2) *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi* 35–42 at 39.

²⁶ Özge Apış, ‘Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri’ (2018) 12(37) *Yasama Dergisi (Kamu Yönetiminde Teknoloji Özel Sayısı II)* 49–86 at 52; Aliusta and Benzer, ‘Siber Suçlar Sözleşmesi’, 39.

²⁷ Aliusta and Benzer, ‘Siber Suçlar Sözleşmesi’, 39.

²⁸ Dülger, ‘Bilişim Suçları’, 453.

²⁹ Oğuz Kaan Pehlivan, *Confronting Cyberespionage under International Law* (New York: Routledge, 2018), 99.

³⁰ *Adli İstatistikler*, 49.

³¹ *Ibid.*, 43. The remaining decisions were decisions regarding jurisdiction, forum or a deferred sentence.

³² Ceza Muhakemesi Kanunu (Turkish Code of Criminal Procedure), Act No. 5271, *Resmî Gazete*, 17 December 2004, numbered 25673.

19.3 COLLECTION OF E-EVIDENCE UNDER TURKISH CRIMINAL PROCEDURE LAW

Under Turkish law, a report or claim related to any crime may be submitted to the office of the prosecutor or to police officers.³³ The public prosecutor, rather than parties, collects evidence.³⁴ Within large cities of Turkey, there are specialised cybercrime bureaus of investigation with specialised prosecutors.³⁵ In many cities, there are also anti-cybercrime departments, which are specialised units of the Turkish police force³⁶ that investigate cybercrime and carry out forensic investigations.³⁷ The lack of a specialised prosecution or police bureau in some cities suggests that some cybercrime victims in Turkey may not have access to the necessary forensic or legal experience.

While Turkish law does not offer a definition for digital evidence, Turkish authorities have various means of collecting it. Investigative measures for interceptions and digital investigations, which are regulated by the CCP and its secondary legislation, are only one way of evidence collection. Mandatory or voluntary cooperation of internet service providers and administrative search and seizure methods used by police forces play a central role in collecting relevant evidence as well. This section will first explain the investigative measures under the CCP and then address the other ways of e-evidence collection.

19.3.1 *Investigative Measures under CCP for the Collection of e-Evidence*

The fifth and sixth parts of the CCP, titled ‘Interception of Correspondence through Telecommunication’ and ‘Undercover Investigator and Surveillance with Technical Devices’, respectively, list a number of investigative measures related to the collection of electronic evidence. These measures are search, copying and provisional seizure of computers, computer programs and transcripts (Article 134); locating, intercepting and recording of correspondence (Article 135); and surveillance with technical means (Article 140). Article 134 of the CCP transposes Article 19 of the CC Convention into the Turkish law; Article 135 of the CCP does the same for Articles 20 and 21 of the CC Convention. Articles 16, 17 and 18 of the CC Convention, however, are not transposed into domestic law.³⁸

Due to clear conflict between the privacy of individuals and the use of interception of conversations or communications or digital investigations, these investigative measures are designed as last resort measures and must be authorised or at least subject to a posteriori control by a judge. Each measure is also subject to detailed conditions and safeguards under the CCP and the Regulation on Judicial and Preventive Searches, which are detailed in Sections 19.3.1.1 and 19.3.1.2.

³³ See, e.g., Article 158 of the CCP.

³⁴ See, e.g., Dr Sezer Gökhan, *A Study on Turkish Criminal Trial* (Ankara: Ankara Bar, 2010), 49 (‘Therefore, in order to find out the truth about the matter and to be able to attain the concept of “fair trial” the Public Prosecutor is required to gather and preserve evidence both in favour of and against the suspect either ex officio or through the judicial police under his authority.’).

³⁵ Council of Europe, ‘Status regarding Budapest Convention’, www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/turkey?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/.

³⁶ According to Article 164 of the CCP, the law enforcement agency (*kolluk*) comprises police, gendarmerie and the coast guard as well as customs officers.

³⁷ See, e.g., ‘Siber Suçlarla Mücadele Daire Başkanlığı’, Emniyet Genel Müdürlüğü, www.egm.gov.tr/siber/hakkimizda2.

³⁸ Yavuz Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi’nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri* (İstanbul: Legal Yayıncılık, 2018), 135.

19.3.1.1 Search, Copying and Provisional Seizure of Computers, Computer Programs and Transcripts (Article 134)

As amended in July 2018, Article 134 of the CCP and Article 17 of the Regulation on Judicial and Preventive Searches³⁹ specify the procedure for searching, copying and seizing computers, computer programs and transcripts.⁴⁰ Unlike the CC Convention, the CCP does not include a definition of a computer (system).⁴¹ The Law on Intellectual Property and Artistic Works defines a *computer program* as a ‘computer command system organised in a way to make a computer system carry out a specific operation or task or preparatory works that would enable the creation or improvement of this command system’.⁴²

The scope of Article 134 of the CCP is narrower than Article 19 of the CC Convention in two respects. Firstly, Article 134 of the CCP relates to ‘search of computers and computer programs and transcripts used *by the suspect*’. Accordingly, the majority of the legal scholars maintain that an Article 134 warrant may be executed only on the suspect’s computer and other computers that may have been used by the suspect.⁴³ Even when there is a tip as to the existence of certain evidence on the suspect’s co-worker’s computer, the police may not search that computer unless they reasonably believe that the suspect used the co-worker’s computer as well.⁴⁴ Article 19 of the CC Convention, however, relates to the search of any computer.

Secondly, Article 19 of the CC Convention foresees search of computer systems and computer-data storage media while Article 134 of the CCP merely refers to ‘*computers*’. Accordingly, it is disputed among scholars whether cell phones or tablets or any other device that processes data would be within the scope of Article 134 of the CCP.⁴⁵ Some scholars argue that the term ‘computers’ should be construed broadly in a way that any device that can perform computing services and store computing data should be within the scope of Article 134 of the CCP,⁴⁶ while others argue that the term should be construed narrowly.⁴⁷ Adopting the second view, the Court of Cassation has ruled that printers were not within the scope of Article 134.⁴⁸

Similarly, legal scholars disagree on the exact meaning of ‘*transcript*’.⁴⁹ While some authors argue that transcript denotes logs, others maintain that it refers to files.⁵⁰ The Court of Cassation seems to side with the latter group, as it offers ‘computer files’ as the English translation of the term transcript.⁵¹

³⁹ Regulation on Judicial and Preventive Searches (*Adli ve Önleme Aramaları Yönetmeliği*) published in the Official Gazette 1 June 2005 and numbered 25832.

⁴⁰ Barış Kalaycı and Filiz Toprak Esin, ‘Amendments to Collection of Electronic Evidence Procedures’, Lexology, 24 September 2018, www.internationallawoffice.com/Newsletters/White-Collar-Crime/Turkey/Gn-Partners/Amendments-to-collection-of-electronic-evidence-procedures?redir=1.

⁴¹ Olgun Değirmenci, *Ceza Muhakemesinde Sayısal (Dijital) Delil* (Ankara: Seçkin, 2014), 32–33.

⁴² See, e.g., Law No. 5846 on Intellectual Property and Artistic Works (*Fikir ve Sanat Eserleri Kanunu*) published in the Official Gazette 13 December 1951 and numbered 7981, Article 1/B(g).

⁴³ Cengiz Tanrıku, *Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma* (Ankara: Adalet Yayınevi, 2014), 447; Erdoğan, ‘Siber Suçlar Sözleşmesi’, 218.

⁴⁴ Tanrıku, ‘Arama ve Elkoyma’, 447.

⁴⁵ Erdoğan, ‘Siber Suçlar Sözleşmesi’, 219.

⁴⁶ See, e.g., Resul Göksoy, *Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenirliliğinin Sağlanması* (Ankara: Seçkin, 2019), 155.

⁴⁷ See, e.g., Şaban Cankat Taşkın, *Bilişim Suçları* (İstanbul: Beta Yayınevi, 2008), 6–7.

⁴⁸ Court of Cassation’s 15th Criminal Chamber, E. 2014/19487, K. 2014/17995, dated 24 November 2014.

⁴⁹ For a summary of different views, see Göksoy, ‘Dijital Delil’, 68; Değirmenci, ‘Dijital Delil’, 52.

⁵⁰ Aslan Ölmez, ‘Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Kopyalama ve Bunlara Elkoyma’ (2009) 4(30) *Terazi Hukuk Dergisi* 45–52 at 46 (arguing that transcripts are logs); Değirmenci, ‘Dijital Delil’, 52 (arguing that transcripts are files).

⁵¹ Court of Cassation’s 16th Criminal Chamber, E. 2015/3, K. 2017/3, dated 24 April 2017.

Under the current version of Article 134 of the CCP, both a judge and, in cases of urgency, a prosecutor may issue a decision on such search, copying and seizure. The decisions rendered by the prosecutor should be submitted for the approval of a judge within twenty-four hours. Upon receiving the approval request, the judge must decide within twenty-four hours whether to approve or annul the decision. In case the judge annuls the decision or fails to render a decision within the designated time period, seized copies and records must be destroyed.

This investigatory measure is designed as a ‘last resort’ measure. That is, a judge or a prosecutor may issue an Article 134 warrant only if there is a strong suspicion of a crime (*kuvvetli şüph*e)⁵² and it is impossible to obtain the evidence in question through other means.⁵³

To offer further protection, Article 134(2) subjects seizure of the suspect’s computer to additional conditions. That is, police may seize the computer only if the computer, computer programs or transcripts are password-protected or forensic analysis of a hard drive (or other computer media) takes too long to perform on site.⁵⁴ In fact, some legal scholars argue that police may also seize additional devices if they would be useful for decryption of the password-protected computer or files.⁵⁵ In practice, however, police officers seize the suspect’s computer even when there is no password protection in place and the search would not take a long time.⁵⁶ Moreover, police officers often do not provide an ‘image copy’ of the hard drive to the suspect, which renders the forensic review prone to abuse. In other words, regrettably, collection of e-evidence through search and seizure of computers is often carried out at the expense of procedural safeguards and fundamental rights. The same applies to the wiretapping measure.

19.3.1.2 Locating, Recording of and Listening to Correspondence (Article 135)

Similar to Article 134 of the CCP, Article 135 is also a ‘last resort’ measure, requiring a strong suspicion that a crime was committed and the impossibility of obtaining evidence through other means. In practice, however, this preventive measure is often used as a measure of first resort, and judges do not exercise strict scrutiny over whether the obtained evidence could have been obtained through other means.⁵⁷

While Article 134 of the CCP regulates ‘retrospective surveillance’,⁵⁸ Article 135 of the CCP sets out the principles and rules of ‘prospective surveillance’.⁵⁹ As in other jurisdictions, it is disputed to which category the interception of emails belongs.⁶⁰ According to the Court of Cassation, emails stored on one’s computer would be intercepted through Article 134 of the CCP, while emails on email services would be intercepted through Article 135 of the CCP.⁶¹

⁵² Özcan Özbey, ‘Adli Bilişim ve Sayısal Deliller’ (2010) 36(3) *Yargıtay Dergisi* 61–126 at 107.

⁵³ Gökhan, ‘Turkish Criminal Trial’, 107.

⁵⁴ Tannıkulu, ‘Arama ve Elkoyma’, 449.

⁵⁵ See, e.g., Veli Özer Özbek, *Ceza Muhakemesi Hukuku* (Ankara: Seçkin, 2006), 359.

⁵⁶ Özbey, ‘Adli Bilişim ve Sayısal Deliller’, 107.

⁵⁷ Marcel Lemonde, *Needs Assessment Report and Recommendations of Action for Turkish Criminal Justice System* (Strasbourg: Council of Europe, December 2013), 106, para. 92 (‘In reality, telephone-tapping is not used as a last resort. On the contrary it is used routinely as the easiest way to investigate crime.’).

⁵⁸ I borrow this term from Orin Kerr who uses retrospective surveillance for search on stored data and prospective surveillance for the surveillance of real-time data. For more detail, see Orin Kerr, ‘The Next Generation Communications Privacy Act’ (2014) 162 *University of Pennsylvania Law Review* 373–419.

⁵⁹ Göksoy, ‘Dijital Delil’, 174.

⁶⁰ Ibid.

⁶¹ Ibid.

Even though the exact wording of Article 135 of the CCP refers to ‘telecommunications’, the provision regulates the interception of wire communications, including landlines, cell phones⁶² or even Skype or WhatsApp calls.⁶³ In order to detect, wiretap, record and examine the conversations of the accused or the suspect,⁶⁴ either a judge or, in cases of emergency, a prosecutor can render a decision to this effect. Like Article 134 of the CCP, the prosecutor’s decision is subject to a judge’s approval subject to the same time limits. However, unlike Article 134 of the CCP, this measure is applicable only to the serious offences enumerated in Article 135 of the CCP, such as torture, homicide, human trafficking and child abuse.

Generally, this investigative measure should not last more than two months. However, a judge may extend the measure for another month in the case of necessity. With respect to offences under investigation or prosecution that involve organised crime, a judge may extend the duration three times, each time for no longer than one month.

While the measure is in progress, no information on the measure should be conveyed to the concerned party. If the prosecutor decides not to prosecute the crime or the judge decides against the decision to monitor the conversations of the suspect or the accused, tape recordings of the conversations should be deleted within a period of ten days.

19.3.1.3 Remote Access to Computers and Communications Abroad

As a natural consequence of the principle of territoriality under public international law, investigative measures under the CCP do not have an extraterritorial effect.⁶⁵ That is, a Turkish court cannot order a physical search of the computers located outside of Turkey; such procedures should be carried out through mutual legal assistance. Yet, secondary laws regarding search of computers and interception of communications create (rather controversial) exceptions to the principle of territoriality.

Neither the CCP nor its secondary legislation explains how search of a computer ought to take place.⁶⁶ Similarly, there is no provision under the CCP as to remote access either.⁶⁷ However, Article 17(3) of the Regulation on Judicial and Preventive Searches sets out the procedure for remote access.⁶⁸ The regulation of remote access allows authorities to conduct searches in the cloud as well.⁶⁹ Article 7(3) of the Regulation on Interceptions of Communication also allows authorities to intercept communications of people abroad.⁷⁰

⁶² Saadet Yüksel, ‘Intelligence Surveillance of Wire Communications under Turkish Law’ (2013) 71(1) *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası* 1313–1326 at 1314.

⁶³ Erdoğan, ‘Siber Suçlar Sözleşmesi’, 276; Göksoy, ‘Dijital Delil’, 174.

⁶⁴ Legal scholars disagree on whether prospective surveillance under Article 135 of the CCP may be utilised during the prosecution phase. Murat Önok, *Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, İletişim Özgürlüğüne Müdahale* (Ankara: Panel, 2009), 51 fn. 9.

⁶⁵ See, e.g., Durmuş Tezcan, Mustafa Ruhan Erdem and Rifat Murat Önok, *Uluslararası Ceza Hukuku*, 5th ed. (Ankara: Seçkin, 2019), 158; *but see* Nur Centel and Hamide Zafer, *Ceza Muhakemesi Hukuku*, 15th ed. (İstanbul: Beta Yayınevi, 2018), 65 (arguing that governments are free to determine ‘how to adjudicate which crimes’ but still concluding that the principle of territoriality applies to the CCP).

⁶⁶ Erdoğan, ‘Siber Suçlar Sözleşmesi’, 221.

⁶⁷ *Ibid.*, 235.

⁶⁸ Regulation on Judicial and Preventive Searches (*Adli ve Önleme Aramaları Yönetmeliği*) published in the Official Gazette 1 June 2005 and numbered 25832, Article 17(3); Erdoğan, ‘Siber Suçlar Sözleşmesi’, 235.

⁶⁹ Erdoğan, ‘Siber Suçlar Sözleşmesi’, 236.

⁷⁰ Regulation on Interceptions of Communication (*Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik*) published in the Official Gazette 14 February 2007 and numbered 26434, Article 7(3); Erdoğan, ‘Siber Suçlar Sözleşmesi’, 276.

The fact that remote access is governed by a *regulation* rather than a law renders this provision unconstitutional, since regulations may not be contrary to the law pursuant to Article 124 of the Turkish Constitution.⁷¹ Some legal scholars argue that, due to the principle of territoriality, both physical and remote access searches may be conducted only on data and computers located within Turkey.⁷² In practice, however, if possible, law enforcement agents resort to remote access. Accordingly, collection of e-evidence through specific e-evidence-related investigative measures goes well beyond the national boundaries of Turkey. The general evidence collection powers of judges and prosecutors seem to follow a similar trend, extending the reach of Turkish judicial authorities to e-evidence located abroad.

19.3.1.4 Prosecutor's Power to Request e-Evidence

According to Article 18 of the CC Convention, competent authorities may order 'a service provider that offers its services in the territory of the party to submit subscriber information relating to such services in that service provider's possession or control'. While Turkish law does not have a corresponding provision, broad powers of prosecutors under the CCP might allow Turkish authorities to reach the same goal.⁷³

Pursuant to Article 332 of the CCP, a judge or a prosecutor may request information from anyone as part of a pending investigation or trial. Unless it is impossible to provide the requested information, the recipients of such a subpoena must comply with it within ten days of receipt. Non-compliance with a subpoena constitutes violation of Article 257 of the TPC (crime of misuse of public duty), which may be sanctioned by up to two years of imprisonment.⁷⁴

Moreover, pursuant to Article 161(1) of the CCP, prosecutors may collect any type of evidence that may shed light on the investigation at issue.⁷⁵ Accordingly, a prosecutor may request the production of certain data from information and communication technology (ICT) companies as well.⁷⁶ In case an ICT company fails to provide such data, a prosecutor may initiate the search procedure under Article 134 of the CCP in relation to that ICT company's servers.⁷⁷

⁷¹ See, e.g., Erdoğan, 'Siber Suçlar Sözleşmesi', 235; Article 124 of the Turkish Constitution reads: 'The President of the Republic, the ministries, and public corporate bodies may issue by-laws in order to ensure the implementation of laws and presidential decrees relating to their jurisdiction, as long as they are not contrary to these laws and decrees.' See Constitution of the Republic of Turkey (*Türkiye Cumhuriyeti Anayasası*) published in the Official Gazette 20 October 1982 and numbered 17844, Article 158.

⁷² Erdoğan, 'Siber Suçlar Sözleşmesi', 236; Osman Gazi Ünal, 'Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma', Master's thesis, Gazi Üniversitesi, 2011, 111; Değirmenci, 'Dijital Delil', 244, 365–366; Göksoy, 'Dijital Delil', 133.

⁷³ Erdoğan, 'Siber Suçlar Sözleşmesi', 181.

⁷⁴ In practice, such short sentences are not served for the period foreseen by a judge, unless the perpetrator commits another crime due to deferral of the announcement of the verdict procedure. See Seyithan Güneş, *Hükmün Açıklanmasının Geri Bırakılması* (İstanbul: On İki Levha Yayıncılık, 2018), 10.

⁷⁵ Erdoğan, 'Siber Suçlar Sözleşmesi', 180:

As a requirement of this obligation imposed on the public prosecutor, Article 161/1 of the Turkish Law of Criminal Procedure clearly states that the public prosecutor can conduct all kinds of investigations. In this case, the public prosecutor may ask persons for a certain data stored in an information system or data storage device under their possession or control. Public prosecutor, in accordance with the provisions of the same law, may also ask service providers to submit their subscription information regarding their services under their possession or control. (translated from Turkish)

See also Göksoy, 'Dijital Delil', 177.

⁷⁶ Göksoy, 'Dijital Delil', 177.

⁷⁷ Ibid.

As for foreign internet service providers, there is no explicit provision that would allow direct contact of the domestic police force with holders of data in foreign jurisdictions.⁷⁸ Moreover, according to an assessment report submitted to the Cybercrime Convention Committee, the Turkish Constitutional Court once ruled that data obtained without an international cooperation commission may not be accepted in legal proceedings.⁷⁹ However, as further elaborated in Section 19.3.3, in practice, prosecutors and police officers frequently contact foreign internet service providers to request data to procure a voluntary cooperation.⁸⁰ Moreover, some of the unlawfully collected e-evidence may even be admissible in court.

19.3.1.5 Probative Value of Unlawfully Collected e-Evidence

Pursuant to Article 267 of the CCP, decisions of judges taken on investigative measures may be subject to a so-called *objection*.⁸¹ The persons affected by such a decision may submit their objection-petition to the criminal judgeship of peace that rendered the decision⁸² within seven days after the execution of the warrant or the execution notice thereof, whichever is earlier.⁸³ If the judge agrees with the objection, he/she may alter or quash the warrant. If not, another criminal judgeship of peace or another competent criminal court will automatically review the decision.⁸⁴ A person who was subject to unlawful search, seizure or wiretapping may seek damages for both material and moral loss.⁸⁵ Whether evidence collected through such unlawful search would be admissible in court, on the other hand, is not always clear.

While the Turkish Constitution and numerous articles of the CCP prohibit the use of illegally obtained evidence in court, the Court of Cassation allows the use of illegally obtained evidence if the illegality is merely due to simple procedural failures.⁸⁶ Following the Court of Cassation's footsteps, judges often analyse whether the procedural failure leads to violation of the

⁷⁸ Cybercrime Convention Committee, *T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime*, T-CY(2013)17rev, 3 December 2014, 120, rm.coe.int/16802e726c ('No explicit prohibition under domestic law. It may depend on the existence of relevant interstate agreements. In practice, data is regularly sought through direct contact.').

⁷⁹ Cybercrime Convention Committee, *T-CY Assessment Report*, 120 ('Data obtained without MLA request is unlikely to be accepted in proceedings, pursuant to a decision by the Turkish Supreme Court on the implementation of Law 2992.'). Surprisingly, I was unable to locate the decision itself, despite seeking help from prominent scholars and practitioners.

⁸⁰ Cybercrime Convention Committee, *T-CY Assessment Report*, 120.

⁸¹ Tanrıkulu, 'Arama ve Elkoyma', 463.

⁸² The criminal judgeships of peace are similar to magistrate judges in other jurisdictions in terms of their authority and obligations. See Venice Commission, *Turkey Criminal Judgeships of Peace Memorandum of the Ministry of Justice*, Opinion No. 852/2016, CDL-REF(2017)004, 8 February 2017, 2, [www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF\(2017\)004-e](https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2017)004-e) ('[T]he criminal judgeships of peace are tasked to decide upon protective measures such as arrest, pre-trial detention, search, seizure, taking under custody, physical examination of the suspect and taking samples from the body.').

⁸³ Erdoğan, 'Siber Suçlar Sözleşmesi', 225.

⁸⁴ Venice Commission, *Memorandum of the Ministry of Justice*, 5 ('In accordance with Article 267 of the Law No. 5271, decisions of judges shall be subject to appeals and there is a procedure regarding effective review of decisions taken on protective measures during the investigations. This procedure is in line with Articles 5, 6 and 13 of the European Convention for Human Rights.').

⁸⁵ Tanrıkulu, 'Arama ve Elkoyma', 465.

⁸⁶ See Court of Cassation's Assembly of Criminal Law Chambers, E. 2005/10, K. 2005/15, dated 15 March 2005; Court of Cassation's Assembly of Criminal Law Chambers, E. 2011/8-278, K. 2012/96, dated 13 March 2012. See also Centel and Zafer, 'Ceza Muhakemesi Hukuku', 796–799; Büşra Demiral Bakırman, 'Unlawfully Obtained Evidences in Turkish Criminal Procedure Law' (2015) 3(1) *Journal of Penal Law and Criminology* 239–248 at 246, <https://dergipark.org.tr/tr/download/article-file/14680> ('For example, performing seizure in a house requires the presence of the public prosecutor. If he or she cannot be present in this search, Art. 119/4 of the CCP says that two persons who can be [are] from [the] community council or neighbour[s] of the house. According [to] this argument in doctrine,

defendant's rights. Hence, Turkish judges may admit unlawfully obtained evidence in cases where they deem that the defendant's rights are unaffected by the illegality.⁸⁷ Emphasising the fact that Article 38(6) of the Constitution does not make a distinction between procedural failures and other kinds of unlawfulness, many legal scholars rightly criticise this interpretation and practice.⁸⁸

It is also not clear whether the fruit of the poisonous tree principle is applicable in Turkish criminal procedure law due to the silence of the CCP on the matter.⁸⁹ While the majority of legal scholars read Article 38(6) of the Turkish Constitution as adopting the principle,⁹⁰ others claim that such a principle may not be applicable unless there is an explicit provision requiring exclusion of unlawfully obtained evidence.⁹¹ The Turkish courts' position on the matter is ambiguous due to decisions adopting both views.⁹²

In light of the Court of Cassation's judgments rejecting the applicability of the fruit of the poisonous tree principle,⁹³ in practice, evidence conducted in an 'illegal' manner may be relied upon. For instance, evidence collected when a procedural step was disregarded, or evidence gathered as a result of earlier illegally obtained evidence, may also be admissible in Turkish courts, posing a threat to the rule of law in Turkey.⁹⁴ This concern becomes more acute considering the recent expansion of police power to collect e-evidence through 'preventive measures' without a judicial control rather than 'investigative measures' subject to a judge's decision.

19.3.2 Rise of Police Powers Regarding e-Evidence

The problems encountered during the collection of e-evidence seem to have led Turkish lawmakers to rely more heavily on 'protective measures'⁹⁵ and to grant more and more power to the police force. For instance, the Police Duties and Competences Law (PDCL), a key piece of legislation for the police force, creates an exception to the general rule that public prosecutors conduct criminal investigations and police officers act under the instructions and orders of the prosecutors. Due to an amendment adopted in 2018 with State of Emergency Decree No. 680,

even if this requirement of the law [is] not fulfilled, the evidence can be used as it has nothing [to do] with violation of fundamental rights and freedoms; it is a simple rule of criminal procedure.'). But see Court of Appeals decisions cited in footnotes 83 and 84 of Centel and Zafer, 'Ceza Muhakemesi Hukuku', 799, for exclusion of all illegally obtained evidence.

⁸⁷ Yusuf Başlar, 'Ceza Yargılamasında Elektronik Delil', PhD thesis, Sakarya Üniversitesi, 2015, 49, <https://acikerisim.sakarya.edu.tr/handle/20.500.12619/77167>.

⁸⁸ Değirmenci, 'Dijital Delil', 422.

⁸⁹ Centel and Zafer, 'Ceza Muhakemesi Hukuku', 799–800.

⁹⁰ Murat Volkan Dülger, *Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğretisi)* (Ankara: Seçkin, 2014), 89.

⁹¹ Başlar, 'Elektronik Delil', 53.

⁹² Centel and Zafer, 'Ceza Muhakemesi Hukuku', 800.

⁹³ Court of Cassation's Assembly of Criminal Law Chambers, E. 2005/7-144, K. 2005/150, dated 29 November 2005 (cited by Yargıtay Kararları Dergisi, vol. 32(3), March 2006, 460–486); Court of Cassation's Assembly of Criminal Law Chambers, E. 2011/8-278, K. 2012/96, dated 13 March 2012.

⁹⁴ Bakırman, 'Unlawfully Obtained Evidences', 246 ('Likewise, the Turkish Appeal Court held this argument and decided that not fulfilling the simple rule in criminal measures does not render the evidence unlawful.').

⁹⁵ Under Turkish law, measures that may be implemented after an offence has been committed are called 'coercive measures', which are referred to in this chapter as investigative measures. The CCP and the Law No. 5651 govern investigative measures. Measures that may be implemented to prevent crimes are called preventive measures (*önleme tedbirleri*). Administrative authorities, such as the police force, are authorised to resort to preventive measures. Apart from the PDCL, the Law on the Gendarmerie Duties and Competences No. 2803 and the State Intelligence Services and the National Intelligence Organisation Act No. 2937 govern preventive measures. See Centel and Zafer, 'Ceza Muhakemesi Hukuku', 436, 444.

pursuant to Supplement Clause 6(18) of the PDCL, when informed of an offence, the police may conduct investigations within cyberspace and determine the identity of the internet user so as to determine the prosecutor of competent jurisdiction. While doing so, the police may request information from content providers, access providers and hosting providers, which are obliged to provide the police with the requested information under the same provision.⁹⁶ Supplement Clause 6(18) of the PDCL was challenged before the Turkish Constitutional Court by the main opposition party in the Turkish parliament and was struck down on the grounds that it violated the legality principle and the right to privacy under the Turkish Constitution.⁹⁷ However, it has often been the practice of the Turkish legislature to re-adopt the provisions struck down by the Constitutional Court verbatim.

The PDCL also authorises the police force to carry out investigations in the cyber realm to maintain security and order. Accordingly, along with carrying out investigations based on complaints, the anti-cybercrimes departments of the Turkish police forces survey approximately 45 million social media users so as to monitor and detect cybercrimes.⁹⁸ Given that there are approximately 60 million internet users in Turkey, it is clear that the scope of such surveillance affects a vast majority of users and a significant proportion of the population of more than 80 million inhabitants.⁹⁹ Thus, the Turkish police may conduct intelligence and evidence gathering on internet users for a seemingly overbroad purpose of *maintaining order and security*. Such power is in conflict with Article 20 of the Turkish Constitution stating that the right to privacy shall not be impeded without a court's order.¹⁰⁰ These powers are also in conflict with the relevant provisions of the CCP that authorise only judges and prosecutors to resort to investigative measures.¹⁰¹ Regardless of such expansion of Turkish law enforcement agents' power, the relevant data may still be out of their reach when stored and protected on servers located outside of Turkey. In such cases, up until the amendment to the Internet Law, which entered into force on 1 October 2020, the Turkish law enforcement agents have relied on the voluntary cooperation of internet service providers. With the introduction of data localisation requirements and hefty fines for failure to cooperate with data requests by the Turkish authorities, the Internet Law may significantly change the means of e-evidence gathering in Turkey.

19.3.3 Cooperation with Internet Service Providers

The Internet Law and its secondary legislation impose obligations on internet actors, such as content providers (Article 4), hosting providers (Article 5) and access providers (Article 6). Under the Internet Law, a content provider is a real or legal person who produces, alters and provides any information or data on the internet while a hosting provider is a real or legal person who

⁹⁶ It was not clear what kind of sanctions would have applied in the case of non-compliance with such subpoenas.

⁹⁷ The Turkish Constitutional Court, E. 2018/91, K. 2020/10 dated 19 February 2020. For the legality principle, see Article 13 of the Turkish Constitution; for the right to privacy, see Article 20 of the Turkish Constitution.

⁹⁸ See Fevzi Kızılkoyun, 'Anti-cybercrime Department Monitors 45 Million Social Media Users in Turkey', *Daily News Hürriyet*, 15 June 2018, www.hurriyetdailynews.com/anti-cybercrime-department-monitors-45-million-social-media-users-in-turkey-133362.

⁹⁹ According to the department, most crimes committed through social media platforms are illegal betting, prostitution and insulting state authorities. In fact, the department has established a special desk to investigate 'insults against state authorities', which closely monitors the social media accounts of the people who refer to the state authorities, see Kızılkoyun, 'Anti-cybercrime Department'.

¹⁰⁰ Ahmet Kurdoğlu, 'Türk Hukukunda ve Avrupa İnsan Hakları Sözleşmesinde Özel Hayatın Gizliliği ve Korunması', Master's thesis, Beykent Üniversitesi, 2018, 47–48.

¹⁰¹ Ibid.

provides the systems containing services and contents, or who operates such systems.¹⁰² By way of example, Facebook, Twitter and YouTube are considered to be hosting providers, while their users who produce content on these platforms are deemed to be content providers. Finally, access providers are defined as real persons or legal entities who provide their users access to the internet, such as TTNET and Türksat in Turkey.

Designed as an independent administrative authority responsible for the regulation and inspection of the telecommunications market, the Information and Communication Technologies Authority (ICTA) enjoys broad powers, one of which is to enact secondary legislation under the Internet Law. It may also request all sorts of data from access and hosting providers.¹⁰³ Access and hosting providers are legally required to submit *any* information requested by ICTA in the requested form and to take *any* requested measure.¹⁰⁴ To be more precise, the provisions in question require compliance with requests made by ICTA with regard to provision of information without any specification as to the type and nature of the information.¹⁰⁵ That is, ICTA may request information without obtaining prior approval or authorisation from prosecutors or courts and in fact may request information from hosting providers without any legitimate reason.¹⁰⁶ Moreover, the Internet Law does not foresee any safeguards or recourses enabling hosting providers to oppose or challenge an order for disclosure.¹⁰⁷ Non-compliance with the information requests is sanctioned with an administrative fine.¹⁰⁸

According to Article 16 of the CC Convention, competent authorities should be able to obtain ‘expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to being lost or modified’. While the applicable provision under Turkish law is not identical to Article 16 of the CC Convention, it may nonetheless produce the same effect.

¹⁰² Ümit Gezder, *İçerik Sağlayıcının ve Yer Sağlayıcının Hukuki Sorumluluğu ve Sorumluluk Muafiyeti* (İstanbul: Beta, 2017), 26, 113.

¹⁰³ See Article 5 of the Internet Law. See also Mehmet Bedii Kaya, ‘The Regulation of Internet Intermediaries under Turkish Law: Is There a Delicate Balance between Rights and Obligations?’ (2016) 32 *Computer Law & Security Review* 759–774 at 767; Dülger, ‘Bilişim Suçları’, 655 (‘This way, ICTA, which is rendered a digital intelligence center, may access all information it may require instantly and with ease. Alongside the fact that no court decision is required to access information, the majority of which constitute personal data, there is no way to know the answers to important questions such as for how long the data in question will be stored, with whom it will be shared and whether it will be destroyed.’) (translated from Turkish).

¹⁰⁴ See, e.g., Articles 5 and 6 of the Internet Law.

¹⁰⁵ Kaya, ‘The Regulation of Internet Intermediaries’, 770; Turgut Kaya, ‘İnternet Servis Sağlayıcının Hukuki ve Cezai Sorumluluğu’, Master’s thesis, Selçuk Üniversitesi, 2019, 133–134.

¹⁰⁶ Kaya, ‘The Regulation of Internet Intermediaries’, 770.

¹⁰⁷ Dülger, ‘Bilişim Suçları’, 656 (‘While the mechanism of objection to sharing the requested information is not provided by law, hosting providers will not object, for the reason that they do not have any interest in sharing the information and there is a sanction for non-compliance with the obligation.’) (translated from Turkish); Kaya, ‘İnternet Servis Sağlayıcıları’, 134.

Based on this clause, [ICTA] may request information from hosting providers without any court decision or legitimate reason. Furthermore, there isn’t any mechanism to object to this request in Turkish Law. Therefore, [ICTA] may arbitrarily request data from the hosting provider at any time or for any reason. This can pose a serious threat to the right of privacy and to the confidentiality of communication. (translated from Turkish).

¹⁰⁸ If a company does not present ICTA with the requested information or documents within the determined period, it will incur an administrative fine of 0.003 per cent of its net sales in the previous year. In the event that the non-compliance with the request is repeated, an increasing fine of up to 1 per cent of the net sales in the previous year applies. Different fines also apply in the event that the documents presented are wrong, missing or falsified. Regulation on Administrative Sanctions by the Information Technologies and Communication Authority (*Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği*) published in the Official Gazette 16 June 2016 and numbered 29744, Articles 23–24.

With seemingly no checks and balances in place, ICTA's data-request powers are worryingly broad in scope.¹⁰⁹ In fact, when Article 5(5) of the Internet Law was initially adopted, the Constitutional Court struck down the relevant paragraph, on the grounds that it violated Article 20(3) of the Turkish Constitution, which foresees the protection of individuals' personal data.¹¹⁰ However, the exact wording of the fifth paragraph was re-adopted by the Turkish parliament after the Constitutional Court's annulment decision.

Accordingly, ICTA may request any type of data from access providers and hosting providers. Such data may end up in criminal courts in two ways. First, Article 279 of the TPC sanctions public officers who fail to report an offence with a penalty of imprisonment for six months to two years. Hence, ICTA officials, who are public officers, are legally required to report an offence if they become aware of it upon requesting data from hosting or content providers. Second, both prosecutors and criminal courts may request ICTA to provide all relevant evidence related to the offence under investigation. In such cases, ICTA may also provide the data that it procured from ICT companies pursuant to the said power.

Similar to data requests, the preservation requirement under the Internet Law is also broad in scope. Pursuant to Article 5 of the Internet Law,¹¹¹ hosting providers are obliged to store traffic information for a period of no less than one year and no more than two years, while the period for access providers for the same shall not be less than six months or more than two years.¹¹² The preservation requirement is more comprehensive than that of the CC Convention. Firstly, unlike Articles 16 and 17 of the CC Convention, the Internet Law requires hosting providers¹¹³ to preserve all traffic data rather than traffic information related to a certain crime.¹¹⁴ Secondly, 'traffic information' under the Internet Law includes subscribers' identity information, which is lacking under the CC Convention.¹¹⁵ Coupled with the data localisation requirement for social media companies, such a broad preservation requirement has significantly broadened Turkish authorities' access to data hosted by ICT companies.

19.3.4 Data Localisation Requirements

The problems encountered by the Turkish judicial authorities and police officers with regard to mutual legal assistance seem to have increased efforts to circumvent judicial cooperation altogether. Frustrated with the lengthiness and the ineffectiveness of these procedures, the

¹⁰⁹ Kaya, 'The Regulation of Internet Intermediaries', 770:

This provision grants [ICTA] a broad margin of discretion, and consequently creates vagueness with regard to the duties and obligations of the ISPs. There are a number of questions which arise from this. Firstly, what kind of information could be requested by [ICTA]? Secondly, what is meant by delivery in the requested form?

Lastly, what kind of measures must the ISPs take in order to fulfil the requirements of [ICTA]?

¹¹⁰ The Turkish Constitutional Court, E. 2014/87, K. 2015/112, dated 8 December 2015, paras. 168–171 ('It is beyond doubt that the provisions subject to the annulment proceeding refer only to "requested information", and as there is no explanatory provision on the matter, *all types of information, which may be associated with specific or specifiable persons, which qualify as "personal data" or "data subject to request" is demandable by [ICTA].*') (translated from Turkish; emphasis added).

¹¹¹ In its *Yildirim v. Turkey* decision, the European Court of Human Rights also ruled that the Internet Law was not in compliance with Article 10 of the European Convention on Human Rights, see *Ahmet Yıldırım v. Turkey*, no. 3111/10, 18 December 2012, hudoc.echr.coe.int/eng-press?i=003-4191041-4965778.

¹¹² Confusingly, however, the Regulation on Broadcasting on the Internet and Fighting Against Crimes Committed through the Internet states that hosting providers should store traffic information for six months. For a criticism of that conflict, see Erdoğan, 'Siber Suçlar Sözleşmesi', 173.

¹¹³ *Ibid.*, 171.

¹¹⁴ *Ibid.*, 174.

¹¹⁵ *Ibid.*

judicial authorities and police officers seem to bypass the international rogatory commission altogether, sending requests directly to the ICT company in question. That is, courts and police officers seem to directly send subpoenas to ICT companies through the mail without even providing a translation of the request letters and without obtaining the approval of the Ministry of Justice.¹¹⁶ While tech giants would be prudent enough to consult their legal advisors before fulfilling these requests, other companies, especially the ones that would not get legal advice to avoid the high legal fees, may nevertheless execute those requests sent without following any of the substantive or procedural safeguards of international judicial assistance.

Perhaps inspired by this *de facto* circumvention of international judicial assistance, the Turkish government has enhanced its data localisation efforts and expanded the extraterritorial application of its law to social media companies so as to create the *de jure* basis for the circumvention.

Prior to July 2020, data localisation requirements under Turkish law were sectoral and limited in scope.¹¹⁷ Introducing a broader data localisation scheme, however, was always on the government's agenda.¹¹⁸ Starting with April 2020, calls for a comprehensive legislation for social media platforms gained momentum.¹¹⁹ The ruling party and its junior coalition partner argued that there was a 'pressing need' to keep social media companies financially and legally accountable.¹²⁰ Such accountability essentially meant circumvention of international judicial assistance, which provided a way to avoid compliance with data requests from Turkey.

Against such a backdrop came the bill proposing to amend the Internet Law in significant ways for social media companies to 'ensure that social media giants follow the rules'.¹²¹ Published in the Official Gazette on 31 July 2020, the amended Internet Law aims to overcome the so-called 'preferential' treatment of foreign ICT companies, by ensuring that they are also subject to applicable Turkish law.¹²²

¹¹⁶ The ICT companies receive a seemingly official government letter (with stamp and signature) only in Turkish.

¹¹⁷ The first major data localisation requirement under Turkish law relates to banks and other financial institutions located in Turkey. The second data localisation requirement relates to electronic communications sectors, such as those using embedded subscriber identity module (e-SIM) technologies. The third important data localisation requirement relates to publicly traded companies, which are also obliged to keep primary and secondary data in Turkey. See Sean Heather, *International Internet Policy Priorities* (Washington, DC: US Chamber of Commerce, 17 July 2018), 5, www.ntia.doc.gov/files/ntia/publications/180717_comments_uscc_ntia_internationalinternetpolicy_priorities.pdf. See also Begüm Yavuzdoğan Okumuş, 'Turkey's BTK Imposes Data Localization Requirements on E-Sim Technologies', Gün+ Partners, 20 May 2019, gun.av.tr/turkeys-btk-imposes-data-localization-requirements-on-e-sim-technologies/; Güniz Gökçe, Ege Güleç, Selin Kaledelen and Seçil Bilgiç, *The Draft Regulation on the Information Systems and Electronic Banking Services of the Banks Announced for Public Consultation* (Levent: GKC Partners, January 2019), http://gkcpartners.com/clients-alerts/The_Draft_Regulation_on_the_Information_Systems.pdf.

¹¹⁸ Daily Sabah with Agencies, 'Turkey's New Social Media Regulations Aim to Provide Safer Platforms for All', *Daily Sabah*, 2 July 2020, www.dailysabah.com/politics/legislation/turkeys-new-social-media-regulations-aim-to-provide-safer-platforms-for-all ('Reform of social media regulations had been on the government's agenda for a long time, with AK Party politicians emphasizing the need for the protection of personal data and reputation.').

¹¹⁹ Emma Sinclair-Webb, 'Turkey Seeks Power to Control Social Media', Human Rights Watch, 13 April 2020, www.hrw.org/news/2020/04/13/turkey-seeks-power-control-social-media.

¹²⁰ Marc Santora, 'Turkey Passes Law Extending Sweeping Powers Over Social Media', *New York Times*, 29 July 2020, www.nytimes.com/2020/07/29/world/europe/turkey-social-media-control.html.

¹²¹ Daily Sabah with Agencies, 'Turkey's New Social Media Regulations' ('The draft legislation prepared by Turkey's ruling party on new social media regulations includes several features to ensure that social media giants follow the rules, provide safer platforms for all users and consider other global examples.') (emphasis added).

¹²² For a more detailed analysis of the obligations of social network providers under the Amended Internet Law, see Seçil Bilgiç, 'Data Localization Law in the Time of Corona: Proposed Amendment to the Law No. 5651', Turkish Law Blog, 14 April 2020.

The current Internet Law requires ‘social network providers’ outside of Turkey that have a daily access of more than 1 million from Turkey to appoint at least one person in Turkey as its representative ‘to ensure compliance with the requirements of services, notifications, or requests’ to be sent by ICTA or the judicial and administrative authorities. Similarly, social network providers, within or outside Turkey, that have a daily access of more than 1 million from Turkey are required to take the necessary measures to *retain the data* of their users located in Turkey within Turkey. The amended Internet Law defines social network providers as ‘real or legal persons that enable users to create, view or share content such as text, images, sound, location on the Internet for social interaction purposes’.¹²³

The representatives and the data localisation requirements for social network providers entered into force on 1 October 2020. All major social media companies in Turkey, such as Facebook, YouTube, Twitter and Pinterest, abided by the new requirement and appointed representatives in Turkey. As of the writing of this chapter, it is not yet clear whether social media companies will host data in Turkey pursuant to Article 4(5) of the amended Internet Law. If social media companies indeed host data in Turkey, it seems that the courts and administrative authorities, such as ICTA, would be able to directly serve data requests to social media companies’ representatives in Turkey, hence bypassing the cumbersome international judicial cooperation step altogether.

This data localisation requirement for social media companies, however, might lead to a further downfall of the freedom of expression in Turkey.¹²⁴ Frequently, the relevant evidence for certain debated criminal offences in Turkey, such as defamation against the president, may be obtained only through international judicial cooperation as the crime is often committed on social media. Hence, relevant electronic evidence regarding many speech crimes is often hosted by tech companies headquartered outside of Turkey, mostly in the US. Having received a request regarding a speech crime, depending on the applicable mutual legal assistance instrument, a requestee country may refuse cooperation if the request (i) does not satisfy the dual criminality requirement (e.g., refusing as defamation against the president is not a crime in that country) or (ii) is not in line with the requestee country’s constitutional protections (e.g., refusing as the prosecution of such libel offence is not in line with the freedom of expression protections under that country’s constitution).

Accordingly, in cases where mutual legal assistance is sought for the prosecution of these speech-related offences, the constitutional protections of the requestee state add another layer of protection of freedom of expression for the defendants in Turkey.¹²⁵ Put differently, initiation of international judicial cooperation before handing in the requested data is akin to using two different sieves with different hole sizes: even if one sieve does not catch an overzealous data request, the other likely will. The data localisation requirements imposed on ICT companies, on the other hand, circumvent the initiation of international judicial cooperation and, hence, subject the data request to only one sieve, the hole size of which is determined solely by the government who produced the data request.¹²⁶ This is why, in the wrong hands, data localisation

¹²³ Ibid.

¹²⁴ For a detailed analysis of the negative correlation between data localisation and freedom of speech, see Secil Bilgic, ‘Something Old, Something New, and Something Moot: The Privacy Crisis under the Cloud Act’ (2018) 32(1) *Harvard Journal of Law & Technology* 348–351. See also Murat Volkan Dülger and Onur Özkan, ‘Sosyal Medya Yasası Meclis’ten Geçti: Peki, Şimdi? [Social Media Law Passed by Parliament: Now What?]', Dülger Hukuk Bürosu, 5 August 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792394.

¹²⁵ For a defendant’s acquittal of the defamation against the president offence (through his posts on Facebook) due to the court’s inability to obtain the related evidence from Facebook through mutual legal assistance, see Ankara Court of Appeals 4th Criminal Chamber, E. 2016/43, K. 2017/67, dated 11 April 2017.

¹²⁶ For an argument against data localisation due to freedom of expression concerns, see Dülger and Özkan, ‘Sosyal Medya Yasası’, 6:

may negatively impact freedom of expression. While there is certainly room for improvement in international judicial cooperation in criminal matters, avoidance of this state-to-state procedure altogether may come at some serious costs.

19.4 INTERNATIONAL JUDICIAL COOPERATION

If the computer that the suspect uses is physically present in Turkey, the prosecutor may ask a judge to issue a search warrant under Article 134 of the CCP. However, if the evidence that the prosecutor wants to collect is located outside of Turkey (and, as explained before, if remote access would not allow the Turkish authorities to collect the relevant e-evidence), international judicial cooperation comes into play. Most of the judicial cooperation requests sent by the Turkish authorities regarding e-evidence concern the internet protocol (IP) addresses or traffic data of the suspects.¹²⁷

Confusingly, under Turkish law, the term ‘rogatory’ is the *chapeau* term for all types of judicial cooperation mechanisms (i.e., for both mutual legal assistance treaties [MLATs] and letter rogatory).¹²⁸ To avoid confusion with the ‘letter rogatory’ term, in this chapter I will use the term mutual legal assistance (MLA) instead.

Under Turkish law only judicial authorities may make or respond to an MLA request. Police officers hence may not make an MLA request but may utilise police cooperation mechanisms. The Ministry of Justice is the Central Authority in international judicial cooperation proceedings.¹²⁹ Within the Ministry, the General Directorate of International Law and Foreign Relations (General Directorate) is the body responsible for the smooth operation of MLA. Judicial authorities may seek international judicial cooperation through three different sources: (i) multilateral MLATs, (ii) bilateral MLATs and (iii) international customary law and the principle of reciprocity.

19.4.1 *Multilateral MLATs to Which Turkey Is a Party*

For Turkish judicial authorities, the most used multilateral MLAT is the European Convention on Mutual Assistance in Criminal Matters (ECMACM),¹³⁰ which has forty-five states parties, including states like Azerbaijan, Armenia and Russia. Turkey signed the treaty on 23 September 1959, ratified it on 24 June 1969 and put it into force on 22 September 1969.¹³¹

Social network providers should not be obliged to store their user data in Turkey, or such an obligation should be regulated in a way that will not make the users sceptical about their privacy. Because fulfilling this obligation may lead to individuals being profiled (tagged) and their social media anonymity would come to an end. It is evident that obliging social network providers to store their user data in Turkey is abuse.

¹²⁷ Dülger, ‘Bilişim Suçları’, 208.

¹²⁸ For the use of ‘rogatory’ to denote judicial assistance in the Ministry of Justice’s official bulletin, see, e.g., ‘Round Table Meeting of the Project on Improving International Judicial Cooperation in Criminal Matters in Türkiye Was Held’ (2022) 26 *International Law Bulletin* 53; Mehmet Salih Az, ‘The Practice of Extradition in the Law of Our Country and Turkish Republic of Northern Cyprus’ (2021) 25 *International Law Bulletin* 11–19 at 11.

¹²⁹ Adalet Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanun (Law on the Organisation and Functions of the Ministry of Justice), Act No. 2992, *Resmî Gazete*, 7 April 1984, numbered 18365, Article 13/A.

¹³⁰ Cybercrime Convention Committee, *T-CY Assessment Report*, 191 (‘Turkey carries out requests of mutual assistance in criminal matters basically within the framework of “European Convention on Mutual Assistance in Criminal Matters”.’).

¹³¹ Kemal Şimşek, *Yabancıların Türkiye’de Yargılanması ve Uluslararası Adli Yardımlaşma* (Ankara: Adalet Yayınları, 2014), 95.

While ratifying ECMACM, Turkey reserved the right to execute a cooperation request pursuant to ECMACM for the search and seizure of property, including data,¹³² dependent on the fulfilment of the three conditions: (a) that the offence motivating the cooperation request is punishable under both the law of the requesting party and the Turkish law; (b) that the offence motivating the cooperation request is an extraditable offence in Turkey; and (c) that execution of the cooperation request is consistent with the Turkish law.¹³³ Other parties to ECMACM may apply reciprocity based on these reservations for requests coming from Turkey.¹³⁴

Albeit slower than many other Council of Europe (CoE) states parties, Turkey has signed and ratified both the First and the Second Additional Protocols to ECMACM as well.¹³⁵ Adoption of the Second Additional Protocol was a criterion that Turkey had to fulfil for its Visa Liberalization Dialogue with the EU.¹³⁶ Unfortunately, the adoption of the Second Additional Protocol was foreshadowed by the freezing of talks between the parties for more than three years. The resumption of the talks came on 22 November 2018 when High Representative for Foreign Affairs and Vice-President of the European Commission Federica Mogherini and Commissioner for European Neighbourhood Policy and Enlargement Negotiations Johannes Hahn met with Turkey's Minister of Foreign Affairs and Chief Negotiator Mevlüt Çavuşoğlu.¹³⁷ To this end, both parties agreed to negotiate for an operational cooperation agreement on the exchange of personal data between Europol and the Turkish authorities competent for fighting serious crime and terrorism.¹³⁸ The talks resumed on 30 November 2018, and their outcome might significantly change the international cooperation landscape for Turkey.¹³⁹ While Turkey has met sixty-five of the seventy-two requirements to achieve the visa liberalisation roadmap, the timeline to see the finish line is still unclear.¹⁴⁰

Though Turkey ratified the CC Convention in September 2014, surprisingly the CC Convention is generally unknown among prosecutors and practitioners. The reason for this might be due to Article 23 ('General Principles Relating to International Co-operation') of the CC Convention, which gives priority to the existing judicial cooperation schemes.¹⁴¹ That is, except in rare cases, the Turkish judicial authorities do not use the mechanisms under the CC

¹³² Council of Europe, *Explanatory Report to the European Convention on Mutual Assistance in Criminal Matters*, ETS No. 30, 20 April 1959, 7 ('The word "property" refers to the "evidence" mentioned in Article 3, paragraph 1.').

¹³³ Şimşek, *Uluslararası Adli Yardımlaşma*, 117.

¹³⁴ John David McClean, *International Co-operation in Civil and Criminal Matters* (Oxford: Oxford University Press, 2002), 178.

¹³⁵ Council of Europe, *Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, ETS No. 99, 17 March 1978; Council of Europe, *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, ETS No. 182, 8 November 2001.

¹³⁶ Republic of Turkey Ministry of Foreign Affairs Directorate for EU Affairs, 'First Meeting of the EU-Turkey Visa Liberalization Dialogue: Agreed Minutes', 16 December 2013, www.ab.gov.tr/files/sib/19_agreed_minutes_ve_annotated_roadmap.pdf.

¹³⁷ Ministry of Foreign Affairs, 'Joint Statement Following the High Level Political Dialogue between the EU and Turkey', 22 November 2018, www.mfa.gov.tr/turkiye-ab-yuksek-duzeyli-siyasi-diyalog-toplantisi_en.en.mfa.

¹³⁸ *Ibid.*, 22.

¹³⁹ Republic of Turkey Ministry of Foreign Affairs Directorate for EU Affairs, 'Negotiations on Draft Agreement between Turkey and the EU on Exchange of Personal Data between the Europol and the Turkish Authorities to Better and Jointly Fight Serious Crimes and Terrorism Were Launched', 3 December 2018, www.ab.gov.tr/negotiations-on-draft-agreement-between-turkey-and-the-eu-on-exchange-of-personal-data-between-the-europol-and-the-turki_51464_en.html.

¹⁴⁰ Republic of Turkey Ministry of Foreign Affairs Directorate for EU Affairs, 'The Visa Liberalization Dialogue', 14 June 2022, [www.ab.gov.tr/the-visa-liberation-dialogue_51819_en.html#:~:text=The%20Visa%20Liberalization%20Dialogue%20\(VLD,stays%20in%20the%20Schengen%20Area](http://www.ab.gov.tr/the-visa-liberation-dialogue_51819_en.html#:~:text=The%20Visa%20Liberalization%20Dialogue%20(VLD,stays%20in%20the%20Schengen%20Area).

¹⁴¹ Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (Geneva: International Telecommunication Union (ITU), 2012), 463; Mütacih Özbeke, 'Avrupa Siber Suçlar Sözleşmesi Çerçevesinde Adli Yardımlaşma', Master's thesis, Galatasaray University, 2015, 151.

Convention; they instead rely on bilateral MLATs or ECMACM. Even though ECMACM does not have a specific clause on the collection of e-evidence, the Turkish judicial authorities seem to rely on ECMACM rather than the CC Convention for their judicial requests as to the collection of e-evidence.¹⁴² Accordingly, the secondary nature of the CC Convention prevents Turkey from reaping the full benefits of being a party to the Convention.¹⁴³

In its 2017 activity record, the Ministry of Justice noted that it is producing a draft law to incorporate the CC Convention.¹⁴⁴ The Minister of Industry and Technology also announced that efforts to incorporate necessary legislative changes to make better use of the CC Convention are underway.¹⁴⁵ It is unclear, however, when this draft law will be available for public review as there was no mention of the draft in the activity records thereafter.

The Ministry of Justice is the Central Authority responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. The point of contact, available twenty-four hours a day, seven days a week, is the Department of Cybercrime of Turkish National Police.¹⁴⁶ Nevertheless, there are efforts to include the General Directorate as the point of contact as well.¹⁴⁷ Unlike its counterparts in many other CC Convention member states, the Turkish twenty-four/seven contact point does not have the competence to send or receive requests for mutual assistance.¹⁴⁸

While ratifying the CC Convention, Turkey issued three reservations and several declarations. Firstly, Turkey reserved the right not to apply the measures referred to in Article 20 ('Real-Time Collection of Traffic Data') and Article 21 ('Interception of Content Data') of the CC Convention to communications being transmitted within a computer system if the system is being operated for the benefit of a closed group of users, does not employ public communications networks and is not connected with any other public or private computer system.¹⁴⁹ The reason for that reservation is to exclude closed computer networks such as Karanet, which is used by the Turkish Army, and Polnet, which is used by the Turkish National Police, from the application of such measures.¹⁵⁰

Secondly, as regards Article 22 ('Jurisdiction') of the Convention, Turkey reserved the right to establish extraterritorial jurisdiction within the scope of Articles 11 and 13 of the Turkish Criminal Law when the offence is committed by a Turkish national outside its sovereign territory.¹⁵¹ Lastly, in accordance with Article 29(4) ('Expedited Preservation of Stored Computer Data') of the Convention, Turkey reserved the right to decline a request for expedited

¹⁴² Şener Mavzer, 'International Cooperation Against Cybercrime', *Cyber Criminology*, 19 November 2014, <http://cybercrimesmavzer.blogspot.com/2014/11/siber-suclarla-mucadelede-uluslar-arasi.html>.

¹⁴³ Analie M. Weber, 'The Council of Europe's Convention on Cybercrime' (2003) 18 *Berkeley Technology Law Journal* 425–446 at 442.

¹⁴⁴ Republic of Turkey Ministry of Justice, *Activity Report for the Year 2017* (February 2018), <https://rayp.adalet.gov.tr/Resimler/1/dosya/rapor2017.pdf>. However, the draft is not available for public review as it has not been signed as a bill yet.

¹⁴⁵ UMED, 'Bilişim, Teknoloji ve Medya Hukuku Paneli Gerçekleştirildi', *Uluslararası Medya Enformasyon Derneği*, 11 July 2020, www.umed.com.tr/bilisim-teknoloji-ve-medya-hukuku-paneli-gerceklestirildi/.

¹⁴⁶ Council of Europe, 'Reservations and Declarations for Treaty No. 185 – Convention on Cybercrime', status as of 7 October 2020, www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/185/declarations; 'Siber Suçlarla Mücadele Daire Başkanlığı'.

¹⁴⁷ Dülger, 'Bilişim Suçları', 2009.

¹⁴⁸ Cybercrime Convention Committee, *T-CY Assessment Report*, 110.

¹⁴⁹ Council of Europe, 'Reservations and Declarations for Treaty No. 185'.

¹⁵⁰ Erdoğan, 'Siber Suçlar Sözleşmesi', 145.

¹⁵¹ Ibid.

preservation of data under this provision in cases where it has reason to believe that dual criminality cannot be fulfilled.¹⁵²

As for its declarations regarding the criminalisation of illegal access, Turkey declared that only offences that were ‘committed by infringing security measures with the intention of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system’ would be within the scope of the CC Convention.¹⁵³ Regarding the criminalisation of computer-related forgery, Turkey declared that only offences that were committed with an intent to defraud or similar dishonest intent would be within the scope of the CC Convention.¹⁵⁴

Currently, the reliance on the CC Convention for the collection of e-evidence is limited. If the bilateral MLAT allows collection of evidence, the Turkish authorities seem to rely on the bilateral MLAT rather than the e-evidence-specific provisions of the CC Convention. Given that a vast majority of relevant e-evidence is stored by US companies (such as messages on WhatsApp, emails exchanged through Gmail, or FaceTime calls using Apple devices), the Turkish judiciary and law enforcement focus more on judicial cooperation mechanisms such as the MLAT with the US.

19.4.2 *Bilateral MLATs to Which Turkey Is a Party*

While Turkey has twenty-seven bilateral MLATs in force, one MLAT is unconditionally the ‘star of the show’. Since many of the major ICT companies are headquartered in the United States, Turkish authorities mostly need the assistance of their US counterparts.¹⁵⁵ The United States and Turkey have one of the oldest MLATs in force, which, moreover, unlike many other ones, also ‘include[s] provisions granting defense counsel permission to access evidence pursuant to an MLAT’.¹⁵⁶

However, structural differences between the two legal systems prevent the Turkish authorities from making the most of the MLAT between the countries. According to an internal circular sent by the General Directorate to prosecutors, the United States frequently rejects requests from Turkish judges and prosecutors due to the nature of the crime.¹⁵⁷ The requests made regarding speech-related crimes are denied by the US authorities, citing freedom of expression under the US Constitution.¹⁵⁸ For instance, defamation against the president is an offence under Turkish law

¹⁵² Ibid.

¹⁵³ Council of Europe, ‘Reservations and Declarations for Treaty No. 185’.

¹⁵⁴ Ibid.

¹⁵⁵ See, e.g., TC Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü [TR Ministry of Justice General Directorate of Foreign Relations and European Union], ‘İnternet Ortamında İşlenen Suçlarda Uluslararası Ceza İstinabe İşlemleri’, <https://diabgm.adalet.gov.tr/Home/SayfaDetay/internet-ortaminda-islenen-suclarda-uluslararası-ceza-istinabe-islemleri14022020041756> (‘Worldwide internet services like Google, Yahoo, Facebook, Skype, Hotmail, Twitter, YouTube have their headquarters in the USA. The cybercrimes committed in our country are mostly perpetrated through these services. We demand the necessary information for legal investigation from American judicial authorities through criminal rogatory means.’) (translated from Turkish).

¹⁵⁶ T. Markus Funk, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges* (Washington, DC: Federal Judicial Center, 2014), 12, www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf (‘The first three MLATs signed by the United States—those with Switzerland, Turkey, and the Netherlands—include provisions granting defense counsel permission to access evidence pursuant to an MLAT. Subsequent MLATs do not include comparable provisions.’).

¹⁵⁷ Merve Erdem and Gürkan Özocak, ‘The Convention on Cybercrimes and Its Impacts on Turkish Law’, Academia.edu, 2016, 21–22, www.academia.edu/36745335/Sinirasan_Bir_Suc_Olarak_Siber_Suclarla_Mucadelede_Uluslararası_Isbirligi.

¹⁵⁸ See, e.g., Ahmet Gül, *Bilişim Suçları*, 2nd ed. (Ankara: Seçkin Yayınları, 2018), 46.

(TPC Article 299). However, the US authorities generally reject requests of evidence regarding the prosecution of this offence pursuant to Article 22 of the US–Turkey MLAT.¹⁵⁹

Another reason why Turkish authorities may not obtain evidence stored by US-based ICT companies is the length of the rogatory commission process. There is no legal requirement for internet service providers in the United States to store the content information of their customers.¹⁶⁰ According to US law, internet service providers must retain electronic documents for only ninety days if they receive a ‘prevention letter’ by the authorities.¹⁶¹ An additional ninety-day extension may apply if government agents request so.¹⁶² However, even in the best-case scenario, retention of the relevant data for 180 days may be too short for the regular time required to process an MLA request.¹⁶³ Data localisation requirements for social media companies may alleviate this problem for Turkish authorities. That is, if social media companies store data belonging to users in Turkey inside Turkey, Turkish authorities could potentially use investigative measures under the CCP (e.g., prosecutors’ authority to request evidence from third parties) rather than the long and often futile MLAT process to collect the relevant e-evidence.

According to the internal circular sent to prosecutors within Turkey regarding rogatory requests (Internal Circular), judicial cooperation requests sent to the US authorities are usually not fulfilled because of the nature of the crime and, relatedly, prosecutorial discretion. The Internal Circular states that low-priority crimes are either not prosecuted or the proceedings for such offences are concluded through a plea bargain in the United States. Per the Internal Circular, the stated rationale for such non-prosecution is the reluctance of the US authorities to allocate resources to prosecute these ‘frivolous’ crimes, since neither the violation nor the loss incurred is significant. Hence, according to the Internal Circular, the US authorities refuse to comply with rogatory requests due to prosecutorial discretion under the US law regarding low-priority crimes. Examples of such crimes pursuant to the Internal Circular include stealing a person’s Facebook password, making online threats, asking for money through using someone else’s social media account and online shopping through stealing someone else’s credit card information.

Frustration at such frequent rejections by the US authorities led to the inclusion of an interesting provision in the Judicial Cooperation Law (which is explained in more detail in Section 19.4.4). Article 3(6) of the Judicial Cooperation Law states that the Central Authority may not send a rogatory request to the relevant country if the request is likely to be rejected.¹⁶⁴ Then-deputy general director of the General Directorate noted that,

[f]or example, where the addressee country fails to fulfil requests for judicial assistance for disputes that fall below a certain level or are summary offences, such as threats, insults or minor

¹⁵⁹ Murat Volkan Dülger and Gözde Modoğlu, ‘Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet ve İletişim Hukuku Uygulama Rehberi (Cybercrimes, Investigations and Trials for Cybercrimes and Internet Telecommunication Law)’, 1 July 2014, 164, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2564591.

¹⁶⁰ Judy Hails, *Criminal Evidence*, 8th ed. (Belmont: Cengage Learning, 2013), 430.

¹⁶¹ H. Marshall Jarrett and Michael W. Bailie, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 3rd ed., OLE Litigation Series (Washington, DC: Office of Legal Education, 2009), 139, www.justice.gov/d9/criminal-ccips/legacy/2015/01/14/ssmanual2009_002.pdf. See also Hails, *Criminal Evidence*, 430; Dülger and Modoğlu, ‘Cybercrimes, Investigations and Trials’, 168.

¹⁶² Hails, *Criminal Evidence*, 430.

¹⁶³ See, e.g., Court of Cassation’s 12th Criminal Chamber, E. 2015/4151, K. 2016/259, dated 13 January 2016 (a futile attempt to request evidence from Facebook due to the ninety-day retention period); Court of Cassation’s 12th Criminal Chamber, E. 2014/1951, K. 2014/18277, dated 22 September 2014; Court of Cassation’s 12th Criminal Chamber, E. 2014/4339, K. 2015/581, dated 19 January 2015; Court of Cassation’s 12th Criminal Chamber, E. 2016/339, K. 2016/4890, dated 23 March 2016.

¹⁶⁴ Abdullah Murat, ‘The Power of the Central Authority in Determination of the Type and Method of Judicial Cooperation’ (2018) 14 *International Law Bulletin* 19–22 at 21.

injuries, forwarding the request to a foreign country would result in loss of time and labor. The Central Authority, which is fully aware of the conduct of the foreign country, may not convey the request to the foreign judicial authority.¹⁶⁵

Exercising this power, the Central Authority rejects many rogatory requests to be sent to the United States regarding defamation, threat or libel crimes. Having encountered too many rejections by the Central Authority, prosecutors also show reluctance to initiate the MLA process to the United States. Reluctance to send an e-evidence-related MLA request increases if there is no applicable bilateral or multilateral MLAT.

19.4.3 *Principle of Reciprocity*

In cases where there are no bilateral or multilateral MLA agreements, judicial cooperation proceedings are executed according to the principle of reciprocity.¹⁶⁶ For instance, since Canada and Turkey are not party to a common MLAT, reciprocity would govern the proceedings.

To determine the existence of reciprocity, the Turkish judicial authorities seek the opinion of the General Directorate.¹⁶⁷ Upon such request, the General Directorate contacts the foreign representative office in that state and evaluates the practices and policy of that jurisdiction based on the information provided.¹⁶⁸ Different chambers of the Court of Cassation disagree regarding the binding nature of the General Directorate's decisions as to reciprocity.¹⁶⁹ That is, while one chamber of the Court of Cassation ruled that a judge is not bound by the reciprocity decision of the General Directorate, the other chamber reasoned that, as the competent and experienced body for international rogatory commission, the General Directorate's view on reciprocity is binding on courts. Such a circuit split may be a reason for a defendant's conviction or acquittal, since it would determine whether the request for judicial cooperation would be accepted. Even if it is true that the General Directorate has an accumulated experience in international judicial cooperation, subjecting courts to the decision of an administrative body admittedly undermines the independence of the judiciary.

19.4.4 *Domestic Law on Judicial Cooperation*

While Turkey has been rich in terms of cooperation treaties, for a long time it lacked a domestic code regulating the field of international judicial cooperation in criminal matters.¹⁷⁰ Scholars often criticised the fact that applicable treaties and rules were dispersed over various sources, and hence were hard to find.¹⁷¹ During this time of legal vacuum, Circular No. 69/2 on 'Matters to Be Paid Attention by Our Judicial Authorities in the International Criminal Rogatory Proceedings' (Circular No. 69/2), published by the General Directorate, was the main text for international rogatory commission.¹⁷²

¹⁶⁵ Ibid.

¹⁶⁶ Faruk Turhan, '6706 Sayılı Cezai Konularda Uluslararası İş Birliği Kanunu'nun Kapsamı ve Genel Hükümleri Hakkında Bir Değerlendirme' (2019) 21 *DEÜ Hukuk Fakültesi Dergisi* 3067–3109 at 3083.

¹⁶⁷ Yavuz Yılmaz, 'Role of Ministry of Justice's Opinion in the Identification of Reciprocity in International Private Law' (2017) 12 *International Law Bulletin* 6–9 at 6–7.

¹⁶⁸ Ibid.

¹⁶⁹ Ibid., 8.

¹⁷⁰ Erdem and Özocak, 'The Convection on Cybercrimes', 4–5.

¹⁷¹ See, e.g., Önok, 'International Co-operation', 1247; Özbek, 'Adli Yardımlaşma', 157.

¹⁷² Turhan, '6706 Sayılı Cezai Konularda Uluslararası', 3069.

The Turkish government responded to the legal scholarship's criticism of the lack of a uniform code on international cooperation¹⁷³ and adopted the Law on International Judicial Cooperation in Criminal Matters (Judicial Cooperation Law) on 23 April 2016.¹⁷⁴ According to the General Directorate, merging all norms into a single piece of legislation, the Judicial Cooperation Law, 'has eased the implementation to a great extent'.¹⁷⁵ However, the brevity of the Judicial Cooperation Law shows that it did not compile all relevant provisions. The Judicial Cooperation Law also does not offer guidance on which MLAT would apply to each of the various cooperation requests. Instead, it merely states general principles of international judicial cooperation, and the applicable norms are still scattered around in various treaties and Directorate circulars. Surprised by the brevity of that law despite its ambitious aim, practitioners and legal scholars expect a secondary legislation that will provide more detailed rules and regulations regarding judicial cooperation.¹⁷⁶

Given the complex and disorderly nature of the current Turkish judicial cooperation law, judges and prosecutors still end up resorting to the wrong or an outdated MLAT, or perhaps do not even go through the international rogatory process when they should have, which prolongs an already lengthy process.¹⁷⁷ For instance, the General Directorate's memorandum on rogatory requests¹⁷⁸ states that both ECMACM and all bilateral MLATs have a (general) dual criminality requirement. This is incorrect. Firstly, the dual criminality requirement under ECMACM applies solely to search and seizures.¹⁷⁹ Secondly, for instance, the bilateral MLAT with the United States does not include a dual criminality requirement.¹⁸⁰ While the Turkish version of that MLAT might have caused some confusion,¹⁸¹ the English version clearly states that grounds

¹⁷³ Republic of Turkey Ministry of Foreign Affairs Directorate for EU Affairs, 'Interview with Mr. Dr. Harun Mert Who Is Appointed as Member of the Court of Cassation' (2018) 15 *International Law Bulletin* 20–24 at 23:

This scattered structure in the legislation was causing different challenges in implementation. The necessity of having a separate law in the field of judicial cooperation was also mentioned in the doctrine. Pursuant to this requirement, within the framework of a project carried out in the Ministry and under the coordination of UHDİGM, the Law on International Judicial Cooperation in Criminal Matters was drawn up and then adopted by the Turkish Grand National Assembly (TGNA) on 23 April 2016 and entered into force upon publication in the Official Gazette on 5 May 2016.

¹⁷⁴ Ministry of Justice Directorate General for International Law and Foreign Relations, 'Cezai Konularda Adli İşbirliği Rehberi', November 2014, 18, <http://diabgm.adalet.gov.tr/Resimler/SayfaDokuman/2492019164244CEZA%C3%8E%20KONULARDA%20ADL%C3%8E%20%C4%B0%C5%9EB%C4%B0RL%C4%B0%C4%9E%C4%B0%20REHBER%C4%Bo.pdf>. See also Council of Europe, *Project Summary: Improving the Efficiency of the Turkish Criminal Justice System* (n.d.), rm.coe.int/16806fi969.

¹⁷⁵ Republic of Turkey Ministry of Foreign Affairs Directorate for EU Affairs, 'Interview with Mr. Dr. Harun Mert', 23.

¹⁷⁶ Turhan, '6706 Sayılı Cezai Konularda Uluslararası', 3080 (arguing that it would be more prudent if the judicial cooperation rules were adopted through a code rather than a secondary legislation).

¹⁷⁷ Requested states reject to cooperate if the request letter refers to the incorrect treaty between the countries or to the principle of reciprocity when there is in fact a treaty between the countries in place. See, e.g., Yavuz Taşolar, 'Cezai Konularda Uluslararası Adli Yardımlaşma Talepleri', *Uluslararası hukuk bülteni*, n.d., 20, https://diabgm.adalet.gov.tr/Resimler/Dokuman/2622020121308fyavuz_tasolar.pdf.

¹⁷⁸ See TC Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü, 'Yabancı Devletlerin İstinabe Taleplerinde Dikkat Edilecek Hususlar', <https://diabgm.adalet.gov.tr/Home/SayfaDetay/yabanci-devletlerin-istinabe-taleplerinde-dikkat-edilecek-hususlar14022020035221>.

¹⁷⁹ Dülger, 'Bilişim Suçları', 205.

¹⁸⁰ Funk, *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges*, 11 ('Unlike extradition treaties enforced in U.S. courts, MLATs do not require dual criminality—that the offense for which the foreign state seeks assistance also constitutes a crime in the requested state.'). Mark A. Rush and Jared A. Kephart, 'Lifting the Veil on the MLAT Process: A Guide to Understanding and Responding to MLA Requests', *Lexology*, 20 January 2017, 6, www.lexology.com/library/detail.aspx?g=dba0c8ef6ce-4af0-af7a-9b812d736248 ('One of the most notable differences between MLATs and extradition treaties is that MLATs generally do not contain a requirement of dual criminality').

¹⁸¹ For authors arguing that the dual criminality requirement exists under Article 22 of the US–Turkey MLAT, see, e.g., Dülger and Modoğlu, 'Cybercrimes, Investigations and Trials', 159.

for refusal are limited to political and purely military offences and sovereignty, security and essential interest exceptions.¹⁸²

Moreover, the General Directorate's website does not mention the CC Convention, the Second Additional Protocol to ECMACM or the Judicial Cooperation Law, which may be one of the reasons why practitioners are unaware of the CC Convention.¹⁸³ Moreover, it misleads the reader on the number of bilateral MLATs that Turkey is party to or the lack thereof. For instance, the General Directorate states that since Turkey and Kosovo do not have a bilateral MLAT, the principle of reciprocity would apply to letters rogatory while, in fact, these countries signed and ratified their Agreement on Mutual Legal Assistance in Criminal Matters in 2013.¹⁸⁴

With such legal vacuums, the evolving character of judicial cooperation in criminal matters on e-evidence is evident. While the General Directorate's efforts to train judges and prosecutors on the matter is remarkable,¹⁸⁵ there is still big room for improvement.¹⁸⁶ This is in plain contrast with the enormous proliferation and speed of initiatives in the area of police cooperation.

19.4.5 Police Cooperation

Turkey has been a member of INTERPOL since 1956; hence, INTERPOL constitutes the most essential pillar of police cooperation for Turkey.¹⁸⁷ Serving under the Ministry of Interior, the Department of Interpol-Europol operates as the Turkish National Central Bureau of Interpol.¹⁸⁸ The Department of Interpol-Europol receives and reviews incoming cooperation requests.¹⁸⁹ The Turkish police fulfil a cooperation request only if the requested action is within the scope of police authorities and the permission of the relevant authorities is obtained.¹⁹⁰ The INTERPOL network may also resort to exchange of information and documents for the prevention of crimes.¹⁹¹

Turkish police forces are working towards increasing the speed and efficiency of their cooperation with their foreign counterparts with two ambitious projects. The first one is the e-Codex Project, which aims to improve the interoperability of the information systems of the judicial authorities within the EU and other participating countries.¹⁹² The second one is the

¹⁸² There may be two reasons why the practitioners came to believe that there is a dual criminality requirement under the US–Turkey MLAT. The first is purely due to interpretation of Article 22(1)(ii). Perhaps due to the phrasing of the sentence in Turkish, some authors read ‘a purely military offense which does not constitute an offense under ordinary criminal law’ as a purely military offence and acts that do not constitute an offence under ordinary criminal law. The second reason may be due to the grounds of refusal stated by the US Department of Justice (DOJ). As explained in Section 19.4.2 of this chapter, the DOJ may refuse to comply with a request if it conflicts with the US Constitution as the MLAT grants such right to refusal when the ‘execution of the request is likely to prejudice its sovereignty, security, or similar essential interests’. Defamation or threat offences under Turkish law would generally conflict with the First Amendment of the US Constitution and, hence, are not offences under US law. Having read such a ground for refusal, Turkish practitioners may summarise the reason as a dual criminality requirement.

¹⁸³ See Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü, ‘Ceza İstinabe’, <https://diabgm.adalet.gov.tr/Home/SayfaDetay/ceza-istinabe14022020012410>.

¹⁸⁴ Agreement between the Government of the Republic of Turkey and the Government of the Republic of Kosovo on Mutual Legal Assistance in Criminal Matters, Prishtina, signed 31 May 2011, ratified 30 April 2013, published in the Official Gazette 22 May 2013, numbered 28654.

¹⁸⁵ Republic of Turkey Ministry of Foreign Affairs Directorate for EU Affairs, ‘Interview with Mr. Dr. Harun Mert’, 22.

¹⁸⁶ Ibid.

¹⁸⁷ Ferhat Güneş, ‘Uluslararası İkili Polis İşbirliğinde İrtibat Görevlilerinin Rolü: Emniyet Müşavirleri ve Emniyet Ataşeleri Örneği’, Master’s thesis, Polis Akademisi, 2013, 99.

¹⁸⁸ Emniyet Genel Müdürlüğü, ‘INTERPOL-EUROPOL Dairesi Başkanlığı’, www.egm.gov.tr/interpol/hakkimizda.

¹⁸⁹ Güneş, ‘Polis İşbirliği’, 19.

¹⁹⁰ Ibid.

¹⁹¹ Ibid.

¹⁹² Maria Angela Biasiotti, Jeanne Pia Mifsud Bonnici, Joe Cannataci and Fabrizio Turchi (eds.), *Handling and Exchanging Electronic Evidence Across Europe* (Cham: Springer, 2018), 24.

e-MLA project of INTERPOL, which aims to create an electronic instrument to request and exchange e-evidence.¹⁹³ Once the e-MLA project is actualised, formal MLA requests will be transferred to INTERPOL's twenty-four/seven networks, in Turkey's case in the Department of Interpol-Europol.

While these efforts to improve and expedite police cooperation are noteworthy, such procedures should not be adopted at the cost of individuals' fundamental rights and freedoms. That is, the real focus of international police cooperation is the prevention of crimes and uncovering crimes before the commencement of judicial processes.¹⁹⁴ For instance, granting more powers to police officers to exchange information to prevent crimes may conflict with individuals' data privacy.¹⁹⁵ Moreover, extending police-to-police cooperation to investigations that occur after an offence has been committed may also conflict with the right to a fair hearing if the courts' involvement in the process stays limited.¹⁹⁶ Notably, it is not clear if the e-evidence procured through police cooperation would be excluded from criminal proceedings. Pursuant to Article 140 of the CCP, if a search or seizure reveals evidence that is not connected to the ongoing investigation or prosecution, the respective police authorities may seize the evidence if there are reasonable grounds of suspicion that another criminal offence was committed. In such cases, the police should immediately secure the evidence and notify the prosecutor.¹⁹⁷ While there is no equivalent rule for e-evidence collected through police cooperation, it would not be unlikely for judges to deem such evidence admissible based on similar grounds. Devoid of the safeguards of investigatory measures and international judicial cooperation, police cooperation should not evolve to become the fast-track access route to e-evidence either for Turkey or for foreign countries.

19.5 ROGATORY REQUESTS FROM FOREIGN STATES

According to the official report of the Ministry of Justice, in the year 2016 the Turkish authorities made 8,709 requests compared to the 2,907 incoming requests that they received.¹⁹⁸ Unfortunately, there are no recent reports of such statistics, but arguably the incoming e-evidence requests to Turkey are still relatively low. Regarding e-evidence requests from foreign countries, Turkey is considered to be responsive and cooperative in executing the requests.¹⁹⁹

The Ministry of Justice, and specifically the General Directorate, serves as the Central Authority with respect to the execution of incoming judicial assistance requests.²⁰⁰ The General Directorate reviews each request based on the applicable multilateral or bilateral MLAT or the principle of reciprocity. Moreover, the General Directorate evaluates whether

¹⁹³ Ibid., 25.

¹⁹⁴ Özbek, 'Adli Yardımlaşma', 45.

¹⁹⁵ Biasiotti et al., *Handling and Exchanging Electronic Evidence*, 92 ('Eventually, the idea to implement key escrow was abandoned after privacy and information security advocates strongly opposed the proposal by emphasising the vulnerabilities it would bring to information systems that malicious third parties could equally exploit.').

¹⁹⁶ See, generally, Stefano Ruggeri, 'Introduction to the Proposal of a European Investigation Order: Due Process Concerns and Open Issues', in Stefano Ruggeri (ed.), *Transnational Evidence and Multicultural Inquiries in Europe* (Cham: Springer, 2014).

¹⁹⁷ Tanrıku, 'Arama ve Elkoyma', 467; Centel and Zafer, 'Ceza Muhakemesi Hukuku', 476–477.

¹⁹⁸ It seems the report is no longer accessible, but it was available in 2019 in the Ministry of Justice, 2016 Report, www.yayin.adalet.gov.tr/dosyalar/diger_yayinlar/sgb/01.pdf.

¹⁹⁹ Dülger, 'Bilişim Suçları', 204; Cybercrime Convention Committee, *T-CY Assessment Report* ('Turkey has a positive approach to judicial cooperation, more precisely; incoming requests are carried out in a flexible and a cooperative manner.').

²⁰⁰ See, e.g., 'V – Matters to Be Paid Attention in the Rogatory Requests of Foreign States', Directorate General for Foreign Relations & EU Affairs, <https://diabgm.adalet.gov.tr/Home/SayfaDetay/ceza-istinabe14022020012410>.

fulfilment of the request would violate Turkish public policy or explicitly conflict with the mandatory rules of Turkey, such as the fundamental rights and freedoms under the Turkish Constitution, and whether the requested state would comply with a request of the same nature. If the General Directorate deems the request ‘unlawful’ based on the aforementioned review, it will return the request to the requesting state.²⁰¹ Moreover, the General Directorate may decline a request if it determines that there is a clear discrepancy between the severity of the offence and the time, labour and expense it would take to fulfil the request.²⁰²

If approved by the General Directorate, the e-evidence request is sent to the appropriate judicial authority or police force.²⁰³ Nevertheless, pursuant to Article 138 of the Turkish Constitution, judicial authorities are not obliged to comply with the request solely because such request is transmitted by the Ministry of Justice, due to the principle of the independence of the judiciary. Judicial authorities indeed go through the same review process as the Directorate, and will fulfil the request only if they deem it to be a lawful one. Judicial authorities wishing to ask for additional documents may contact the General Directorate. The judicial authority rejecting the cooperation request should transmit the rejection letter to the General Directorate as well.²⁰⁴ For search or seizure requests, the General Directorate and judicial authorities should also confirm that the requesting state is legally authorised to carry out the procedure under its own law.

Ordinarily, Turkey will meet the costs of executing a request, except for costs of an extraordinary nature.²⁰⁵ However, a partial or complete reimbursement by the requesting state may be asked if the expense is related to (i) expert fees, translation fees and reimbursement of witnesses for travel expenses; (ii) expenses connected to the storage and delivery of objects; and (iii) expenses related to the use of visual or audio communication technologies.²⁰⁶

Perhaps due to the relatively low number of incoming cooperation requests, the domestic rules on responding to such requests are not robust. The explanations provided in part 5 are applied *mutatis mutandis*. Turkish law on direct requests to Turkish ICT companies remains underdeveloped as well.²⁰⁷ There is no specific law allowing or prohibiting foreign law enforcement authorities to contact Turkish ICT companies to request evidence.²⁰⁸ Naturally, there is no distinction between the disclosure of content and non-content data. Thus, in theory, Turkish ICT companies may be voluntarily disclosing data to foreign judicial and law enforcement authorities, while companies facing such requests will surely make evaluations under the Turkish Data Protection Law.²⁰⁹ The applicable laws are silent as to who would bear the costs of such direct e-evidence requests to Turkish companies.

²⁰¹ ‘Cezai Konularda Adli İşbirliği Rehberi’, 30.

²⁰² Article 3(6) of the Judicial Cooperation Law; Murat, ‘The Power of the Central Authority’, 20.

²⁰³ Murat, ‘The Power of the Central Authority’, 20.

²⁰⁴ Ibid.

²⁰⁵ Dülger, ‘Bilişim Suçları’, 204.

²⁰⁶ Ibid.

²⁰⁷ Cybercrime Convention Committee (T-CY) Cloud Evidence Group, ‘Emergency Requests for the Immediate Disclosure of Data Stored in Another Jurisdiction through Mutual Legal Assistance Channels or through Direct Requests to Service Providers’, 20 May 2016, 21, 24, 30, <https://rm.coe.int/1680651a6f>.

²⁰⁸ Ibid.

²⁰⁹ Turkey’s self-reports, available in the CC Convention’s T-CY Reports, seem to be stating that direct contact of Turkish ICT companies by foreign authorities is not possible. While there is no specific legal mechanism for such contact, without an explicit prohibition on voluntary disclosure, Turkish ICT companies may be voluntarily disclosing traffic or content data. See, e.g., Cybercrime Convention Committee, *T-CY Assessment Report*, 120.

19.6 CONCLUSION

Technology has transformed our lives and it certainly has transformed criminal proceedings. Even when both the victim and the suspect are Turkish nationals residing in Turkey, the judicial authorities may have to initiate international rogatory proceedings if the necessary piece of evidence is considered to be abroad. Put differently, international judicial cooperation is an essential piece of contemporary criminal proceedings.²¹⁰

Party to twenty-seven bilateral and seventeen multilateral MLATs, *on paper*, Turkey is well integrated in the international judicial cooperation network. *In practice*, however, as explained earlier, the MLATs do not always guarantee access to e-evidence. Turkish authorities' access to e-evidence located outside of Turkey therefore may be limited. However, the Turkish authorities attempt to overcome such access problems through remotely accessing servers outside of Turkey and broadening the powers of ICTA.

These efforts to reach inculpatory evidence may have already started to pay dividends as the percentage of convictions increased by 13.5 percentage points between 2014 and 2021.²¹¹ According to the official judicial statistics, in the year 2021, 50.6 per cent of all criminal trials resulted in conviction, while only 15.0 per cent resulted in acquittal.²¹² The same statistics were 47.5 per cent and 15.0 per cent in 2020, respectively.²¹³ Given the prevalence of e-evidence in contemporary trials, one may hypothesise that such an increase is due to an improvement in Turkish judicial authorities' ability to collect relevant e-evidence.

Against such a backdrop, it will be worthwhile to understand the impact of the newly appointed representatives of social media companies and the implementation of the new data localisation requirements on criminal proceedings. In a conservative estimate, speech-related crimes constituted 21.4 per cent and 21.0 per cent of all reported offences in Turkey in the years 2020 and 2021, respectively.²¹⁴ Put differently, one in five reported offences in Turkey (if not more) could be classified as speech-related crimes. Given the near-ubiquitous use of social media, the cooperation of social media companies may impact such statistics. As the global champion of issuing take-down requests to social media companies, Turkey's voluntary cooperation requests to access e-evidence regarding speech-related crimes have hitherto been politely declined. It will be interesting to observe if the amended Internet Law will convince or coerce foreign social media companies to cooperate more with the Turkish judicial and law enforcement authorities. Against the backdrop of already robust powers to collect e-evidence located in Turkey, such voluntary cooperation may enable greater surveillance by the Turkish authorities of journalists, human rights defenders and opposition voices.²¹⁵

²¹⁰ Tanrıku, 'Arama ve Elkoyma', 261.

²¹¹ 'Adli İstatistikler', 36.

²¹² Ibid. The remaining decisions relate to forum, jurisdiction or deferred judgments.

²¹³ Ibid.

²¹⁴ Ibid., 21.

²¹⁵ Article 19, 'Turkey: Twitter Becomes Latest Company to Comply with Repressive Social Media Law', 24 March 2021, www.article19.org/resources/turkey-twitter-becomes-latest-company-to-comply-with-repressive-social-media-law/.

Obtaining Digital Evidence under UK Law

Elif Mendos Kuşkonmaz and Ian Walden

20.1 INTRODUCTION

This chapter examines the legal landscape around the investigatory powers of UK law enforcement authorities (LEAs) and the duties of service providers to cooperate with them. The LEAs derive their investigatory powers to obtain digital evidence from a web of UK legislation. At the centre of this web is the Investigatory Powers Act 2016 (IPA), which governs the powers of the LEAs (including the security and intelligence services) to obtain information using different measures. For this reason, this chapter starts by considering the terminology and the categorisation of data provided by the IPA before considering the data retention obligations of service providers. Next, the chapter sketches the rules and procedures for the investigatory powers of LEAs found in other statutes to provide a comprehensive framework for cooperation between service providers and LEAs in obtaining digital evidence. We conclude by providing an overview of the cooperation of LEAs with non-UK-based service providers and of UK-based service providers with foreign LEAs.

20.2 TERMINOLOGY AND CATEGORISATIONS

20.2.1 *Data*

The IPA introduces an array of different types of data that LEAs may obtain by multiple coercive powers. This subsection explores the categories of data that are most crucial in collecting digital evidence.

Central to the IPA is the difference between ‘content data’¹ and ‘communications data’² because access to either data type triggers different rules. Access to content is governed by the interception regime, which requires an interception warrant under the IPA to obtain communications content either in transmission or when stored by the service provider.³

Possibly, the type of data defined under the IPA that is most complex to understand is ‘communications data’. This type of data is defined through overlapping subcategories of communications data, including such categories as ‘systems data’,⁴ ‘relevant communications

¹ Investigatory Powers Act 2016 (IPA), s. 263(6).

² IPA, s. 263(5). It should be noted that various parts of the IPA were amended in 2024 (see the Investigatory Powers (Amendment) Act 2024). At the time of finalising this chapter, the new Act was not yet in force.

³ See Sections 20.4.3.1 and 20.4.3.2 of this chapter. *R v. A, B, D, C* [2021] EWCA Crim 128. This is because interception under this Act can take place if the content of the communication is made available at a ‘relevant time’ (IPA, s. 4(4)). That time is either during the transmission of a communication or any time when it is stored in or by the provider.

⁴ IPA, s. 263(4).

data'⁵ (which comprises 'events data' and 'entity data'), 'internet connection records' (ICR),⁶ 'secondary data'⁷ and 'equipment data'⁸ (which may include 'identifying data' or 'related systems data').⁹ The focal point of these subcategories, particularly concerning the UK system on data access and data retention, is the division between 'events data' and 'entity data'.

'Events data' means any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time.¹⁰ This data category covers information regarding when a message has been sent or received, the location where a person has made a phone call or has sent an email, Wi-Fi hotspots through which someone has connected online or the internet protocol (IP) address of the intended receiver.¹¹ In this context, the government is of the view that traffic and location data, as defined in the e-Privacy Directive (which is implemented in UK law by the Privacy and Electronic Communications (EC Directive) Regulations 2003 and retained post-Brexit), falls within the definition of events data.¹² According to the government, these types of data differ from subscriber data, which is covered by the definition of entity data.¹³

Entity data as a subcategory of communications data means any data which is about an entity (i.e., a person or a thing) or an association between a telecommunication system (or any part of

⁵ IPA, s. 87(11).

⁶ IPA, s. 62(7)(a)–(b).

⁷ IPA, s. 16(4).

⁸ IPA, s. 100.

⁹ Section 261(5) of the IPA states:

"Communications data" . . . means entity data or events data —

(a) which is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator and —

is about an entity to which a telecommunications service is provided and relates to the provision of the service,

is comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted, or

does not fall within sub-paragraph (i) or (ii) but does relate to the use of a telecommunications service or a telecommunication system,

(b) which is available directly from a telecommunication system and falls within sub-paragraph (ii) of paragraph (a), or

(c) which —

(i) is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator,

(ii) is about the architecture of a telecommunication system, and

(iii) is not about a specific person,

but does not include any content of a communication or anything which, in the absence of subsection (6)

(b), would be content of a communication.

See views on the complexity of the definitions of communications data in Lorna Woods, 'Draft Investigatory Powers Bill' (2016) 2 *European Data Protection Law* 103; Investigatory Powers Commissioner's Office (IPCO) and Office for Communications Data Authorisations (OCDa), *Annual Report of the Investigatory Powers Commissioner 2020* (6 January 2022), 90, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPCO-Annual-Report-2020_Web-Accessible-version.pdf.

¹⁰ IPA, s. 261(4).

¹¹ Home Office, *Communications Data Code of Practice* (November 2018), paras. 2.44–2.45, pp. 14–15, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf.

¹² Home Office, 'Investigatory Powers Act 2016: Consultation on the Government's Proposed Response to the Ruling of the Court of Justice of the European Union on 21 December 2016 Regarding the Retention of Communications Data', November 2017, 10, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663668/November_2017_IPA_Consultation_-_consultation_document.pdf.

¹³ Home Office, 'Investigatory Powers Act 2016', para. 2.34, p. 12.

it) and an entity.¹⁴ To fall within the definition of entity data, the relevant data must consist of or include data which identifies or describes the entity (*whether or not by reference to the entity's location*), and is not events data.¹⁵ This definition covers data identifiers associated with communication (i.e., subscriber data), such as phone numbers or IP addresses allocated to an individual¹⁶ or routers; information about the person using the service, such as email address; information about the devices; and information on the services to which users subscribe, such as mobile phone applications or internet subscriber services installed on mobile phones.¹⁷ Moreover, it may also cover subscribers' passwords.¹⁸ However, to use the password obtained to access the content of any stored communications, a LEA must ensure that it has appropriate lawful authority for the interception regime.¹⁹

A controversial aspect of entity data is the reference in its definition to the entity's location. This reference triggered questions during the 2017 consultation on changes to the IPA post-*Tele2* on the extent to which the different purposes (i.e., the prevention and investigation of crime or serious crime) for retaining entity data, on the one hand, and events data, on the other, satisfy the *Tele2* requirements.²⁰ The position of the government during this consultation was that these requirements applied to events data as it comprises traffic and location, data the retention of which were subject to a legal dispute in *Tele2*, and did not apply to entity data.²¹ As explained in Section 20.3.2.1.2 of this chapter, following *Tele2*, the Court of Justice of the European Union (CJEU) has adopted a more nuanced approach in considering the permissibility of retaining different categories of communications data.²²

In addition to the above categorisations of entity data and events data, two definitions are important for communications data as set out in the IPA. The first definition is that of 'data' because it is the precursor for each subcategory. Accordingly, this term is defined very broadly

¹⁴ IPA, s. 261(3).

¹⁵ Ibid. [emphasis added].

¹⁶ The *Communications Data Code of Practice* mentions:

There are some circumstances where a telecommunications operator will need to process events data in order to respond to a request for entity data. In such circumstances, the level of authorisation required is for the type of data that is to be disclosed, rather than the type of data that is processed e.g., where a public authority wants to know the identity of a person using an IP address at a specific time and date this will be an application for entity data.

See Home Office, *Communications Data Code of Practice*, para. 2.36, p. 13.

¹⁷ Ibid., para. 2.41, p. 14.

¹⁸ Ibid., para. 2.42, p. 14.

¹⁹ Ibid. The interception regime and the admissibility of evidence obtained through an interception warrant and an equipment interference are discussed in Sections 20.4.3.1 and 20.4.3.2.

²⁰ Big Brother Watch, 'Big Brother Watch's Response to the Government's Consultation on the Ruling of the Court of Justice of the European Union on 21 December 2016 Regarding the Retention and Acquisition of Communications Data', January 2018, 10, <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/01/Big-Brother-Watch-Response-to-the-Watson-Consultation-Jan-2018.pdf>; Liberty, 'Liberty's Response to the Government's Consultation on the Ruling of the Court of Justice of the European Union on 21 December 2016 Regarding the Retention and Acquisition of Communications Data (Proposed Amendments to the Investigatory Powers Act 2016 and Communications Data Code of Practice)', 18 January 2018, 5, www.libertyhumanrights.org.uk/wp-content/uploads/2021/04/2018.01.18-liberty-consultation-response-FINAL.pdf.

²¹ Home Office, 'Investigatory Powers Act 2016', 10–11.

²² Case C-207/16 *Ministerio Fiscal* [2018] ECLI:EU:C:2018:788; Case C-623/17 *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others* [2020] ECLI:EU:C:2020:790; Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v. Premier Ministre and Others* [2020] ECLI:EU:C:2020:791. Post-Brexit, the UK courts should use these decisions as interpretive tools when determining UK law based on unmodified retained EU law, e.g., the IPA and the Privacy and Electronic Communications Regulation 2003. See European Union (Withdrawal) Act 2018, s. 6.

under the IPA to cover non-electronic data (e.g., paper records).²³ The reason for this broad definition is to prevent circumvention of the regime by not having information in electronic form. The second definition is of ICR, which, as mentioned earlier, is a subcategory of communications data.

The subcategory ICR is defined as communications data that may be used to identify a telecommunication service through which a communication is transmitted to obtain access to, or to run, a computer file or computer program.²⁴ It comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person).²⁵ This specific category of communications data is designed to cover machine-to-machine data. Thus, it can identify specific services or applications that a user has connected to (e.g., WhatsApp) when accessing the internet through their internet access service (e.g., broadband internet connection, public Wi-Fi).²⁶ It can also encompass internet browsing history.²⁷ As explored in Section 20.3.2.1.3, the access regime to ICR records requires different conditions.²⁸

20.2.2 Service Providers

The IPA defines service providers who may have duties to cooperate with LEAs broadly. Article 261(10) provides two conditions that define ‘telecommunications operators’ who may have cooperation duties: (i) where a person offers or provides ‘telecommunication services’ to persons in the UK and (ii) where a person controls or provides a telecommunication system which is (wholly or partly) in the UK or controlled from the UK.²⁹ The breadth of these conditions results in the extraterritorial application of the IPA. It can, therefore, give rise to conflict of laws situations for a telecommunications operator between the UK and the jurisdiction in which it is based (see further Section 20.5.2.3).

A telecommunications service is defined in the IPA as ‘any service that consists in the provision of access to and of facilities for making use of any telecommunication system, whether or not provided by the person providing the service’.³⁰ The Act further clarifies that this includes ‘any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system’.³¹ This means the definition covers internet-based services such as over-the-top (OTT) services (i.e., Skype), web-based email, messaging applications and cloud-based services.³²

²³ According to s. 263(1) of the IPA, data ‘includes data which is not electronic data and any information (whether or not electronic)’.

²⁴ IPA, s. 62(7)(a).

²⁵ IPA, s. 62(7)(b).

²⁶ Home Office, *Communications Data Code of Practice*, para. 2.74, p. 19.

²⁷ *Ibid.*, para. 2.77, p. 20.

²⁸ The different legal purposes applicable to obtaining access to ICR have raised questions on imposing less restrictive conditions for a set of data, access to which may reveal information more than communications between two endpoints in the cases of uniform resource locator (URL) addresses. See Graham Smith, ‘The Coming UK Surveillance Debate: Communications Data Retention, Part 3’, Cyberleagle, 12 August 2015, www.cyberleagle.com/2015/08/the-coming-uk-surveillance-debate_g2.html.

²⁹ IPA, s. 261(10). The definition will be amended by the Investigatory Powers (Amendment) Act 2024, s. 19.

³⁰ IPA, s. 261(11).

³¹ IPA, s. 261(12).

³² Home Office, ‘Interception of Communications Code of Practice’, March 2018, para. 2.6, p. 11, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

The term ‘telecommunications system’ means ‘a system (including the apparatus comprised in it) that exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy’.³³ Under the Communications Act 2003, a person may control a system even though he or she may not have ownership over it.³⁴

20.3 SETTING THE SCENE

20.3.1 *General Approach to the Collection of Digital Evidence*

Currently, UK law does not provide specific rules for seizing, presenting and retaining evidence stored in digital devices. For this reason, digital evidence is subject to the same rules and laws that apply to documentary evidence.³⁵ There is a guidance note (Guidance) published by the then Association of Chief Police Officers (ACPO) that provides guidance on identifying, preserving and recovering digital evidence.³⁶ It aims to demonstrate good practice for recovering electronic evidence from digital devices rather than to substantiate the examination of that evidence. It identifies items that may be seized (e.g., monitors, modems, routers, memory sticks) and procedures that should be followed to preserve the integrity of the stored evidence. The Guidance is based on four principles:

- (i) No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.
- (ii) In circumstances where a person finds it necessary to access original data held on a computer or storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- (iii) An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- (iv) The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

The Guidance focuses on the retrieval of evidence from computers, but also considers retrieving evidence from the internet, such as capturing live website content, or from emails.

The absence of specific rules relating to digital evidence raises issues regarding the transparency of how it is recovered and the compliance of the police with data protection principles when gathering it (particularly with regard to compliance with the principle of proportionality).³⁷ However, insofar as evidence comprises personal data within the meaning

³³ IPA, s. 261(13).

³⁴ Communications Act 2003, s. 32(4)(b).

³⁵ Police and Criminal Evidence Act 1984 (PACE), s. 78. See also Section 20.4.2 of this chapter.

³⁶ Association of Chief Police Officers (ACPO), *ACPO Good Practice Guide for Computer-Based Digital Evidence* (October 2011), www.npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf.

³⁷ With regard to the transparency problem, the report of November 2017 by Big Brother Watch UK – a non-governmental organisation working on the protection of privacy and civil liberties in the UK – showed that the police were not able to provide information on the number of devices seized and the amount of evidence extracted from the seized devices. However, the observations in this report are limited to PACE 1984. Big Brother Watch, ‘Police Access to Digital Evidence’, November 2017, <https://bigbrotherwatch.org.uk/wp-content/uploads/2017/11/Police-Access-to-Digital-Evidence-1.pdf>.

of the Data Protection Act 2018 (DPA), LEAs have to process the information in line with the data protection principles in the context of law enforcement purposes under the Act.³⁸

20.3.2 Data Retention Obligations: Legal Framework, Practice and Challenges

This section focuses on the rules under the IPA on access to and retention of communications data. It follows the structure of the IPA, which first sets out the procedures for acquiring communications data and details the procedures for requiring the retention of communication data by telecommunications operators. The access rules are applicable regardless of whether the data has been retained under the data retention regime. This section covers only the ‘targeted’ regime for access to communications data. There is a separate regime for acquiring communications data in ‘bulk’, but these powers are granted only to the intelligence and security services, which are outside the scope of this chapter.³⁹ The ‘targeted’ regime, as opposed to the ‘bulk’ regime, is a terminology the IPA uses to differentiate procedures and standards applicable to both regimes.

20.3.2.1 Access to Data

Part 3 of the IPA provides the rules for access to communications data. Two types of person may authorise the obtaining of communications data: (i) an officer from the Office for Communications Data Authorisation (OCDA)⁴⁰ or (ii) a designated senior officer (DSO) of a ‘relevant public authority’ listed in Schedule 4.⁴¹ An authorisation allows officers within a public authority to issue a notice to telecommunications operators to obtain and disclose the required data or engage in conduct to acquire it themselves.⁴² As mentioned in Section 20.2.1, the rules on access to communications data changed post-*Tele2*. As a result, the procedures for authorisation by the two authorities (i.e., DSO and OCDA) coexist with slight changes in the purposes for which authorisation can be made. Finally, local authorities such as district councils may also seek access to communications data, as relevant public authorities, but a different set of rules applies to their authorisations.⁴³ For example, they cannot request access to ICR.⁴⁴

This section will explore the rules for authorising an OCDA officer to obtain communications data, before moving on to the general requirements for authorising access to communications data by DSOs. Next, the section covers the specific rules that apply to authorisation for obtaining ICR and the role of single points of contact (SPoC) in the authorisation process.

20.3.2.1.1 THE POWER OF AN OCDA OFFICER TO AUTHORISE OBTAINING OF COMMUNICATIONS DATA. Post-*Tele2*, the IPA was amended to introduce section 60A, which designated the Investigatory Powers Commissioner (IPC) as the person to authorise obtaining

³⁸ Data Protection Act 2018 (DPA), Part 3. See also Section 20.5.2.4 of this chapter.

³⁹ For example, Part 5 of the IPA addresses the equipment interference whereby the LEAs or intelligence agencies (i.e., MI6 and GCHQ) access a device, system or network. Part 6 of the Act provides bulk investigative powers (i.e., powers to oblige service providers to intercept overseas-related communication, retain communications data or give access to such data, and interfere with the device without a target) to intelligence agencies in the context of investigations of serious crimes.

⁴⁰ IPA, s. 60A.

⁴¹ IPA, ss. 61–61A.

⁴² Home Office, *Communications Data Code of Practice*, para. 6.1, p. 41.

⁴³ IPA, s. 86(2).

⁴⁴ IPA, s. 73 (on local authorities’ power to request access to communications data) and see s. 62 of the IPA (on limitations for access to ICR).

communications data requested by public authorities. The IPC was introduced to replace the previous three oversight bodies (i.e., the Interception of Communications Commissioner, the Office of Surveillance Commissioners and the Intelligence and Security Committee) and is tasked with authorisation and review duties.⁴⁵ Among these duties, the IPC deferred its power to authorise the acquisition of communications data to the OCDA, which commenced its role in April 2019. The purposes for which an officer of the OCDA may authorise obtaining of communications data are (i) national security interests, (ii) the applicable crime purpose, (iii) the interests of the economic well-being of the UK insofar as those interests are also relevant to the interests of national security, (iv) public safety interests, (v) prevention of death or injury, (vi) the assistance of investigations in alleged miscarriages of injustices, or (vii) identifying missing persons.⁴⁶ As will be explained in Section 20.3.2.1.2, DSOs may also have the power to authorise access to communications data for the first three purposes.⁴⁷

Finally, as mentioned earlier, local authorities may seek access to communications data.⁴⁸ Access by local authorities is no longer subject to judicial approval, as was required before the 2018 amendments, although it must be approved by an officer of the OCDA.⁴⁹ Local authorities can request access to communications data for ‘applicable crime’ purposes.⁵⁰ This means they can make such requests to detect and prevent crime or public disorder if the required communication is not events data.⁵¹ If the required data is events data, they can make such requests only to prevent and detect serious crime. They cannot make access requests to obtain ICR.⁵²

20.3.2.1.2 THE POWER OF A DSO TO AUTHORISE OBTAINING OF COMMUNICATIONS DATA. As regards the DSOs of public authorities,⁵³ Schedule 4 of the IPA provides a table that sets out a detailed list of the relevant public authorities; the minimum office, rank or position of the DSO in each such authority; and the type of communications data that may be requested (i.e., entity data or all). Overall, all DSOs can grant authorisation if three main requirements are met.⁵⁴ These requirements are: (i) the authorisation must be necessary for a statutory purpose; (ii) it must be necessary for a specific investigation or a specific investigation related to these statutory purposes; and (iii) it must be proportionate to the purpose for which access is sought.

Among these requirements, the requirement to access data based on a statutory purpose has been the most controversial one. Accordingly, for a DSO to grant authorisation for obtaining communications data, that authorisation must be necessary for the statutory purposes laid out in s. 61(7), which are narrower than the purposes for which an OCDA officer may make authorisations under s. 60A. These purposes are national security interests, ‘the applicable crime purpose’ or the interests of the economic well-being of the UK insofar as those interests are also relevant to the interests of national security. When the IPA was first enacted, authorisation could be made based on a wide array of other purposes, such as protecting

⁴⁵ IPA, Part 8.

⁴⁶ IPA, s. 60A(7).

⁴⁷ Home Office, *Communications Data Code of Practice*, para. 5.17, p. 36.

⁴⁸ IPA, s. 73.

⁴⁹ IPA, s. 75.

⁵⁰ IPA, s. 73(3).

⁵¹ *Ibid.*

⁵² IPA, s. 62(A1).

⁵³ According to s. 263(1) of the IPA, public authority means a public authority within the meaning of section 6 of the Human Rights Act 1998, other than a court or tribunal.

⁵⁴ For a more detailed discussion on the authorisation procedure, see Simon McKay, *Blackstone's Guide to the Investigatory Powers Act 2016* (Oxford: Oxford University Press, 2017), paras 4.12–4.20, pp. 83–84.

public health and assessing and collecting tax. Post-*Tele2*, the Act was amended to limit these purposes to those currently listed in s. 61(7).

The statutory ‘applicable crime’ purpose introduced post-*Tele2* raised several concerns when it was introduced as part of the 2018 amendments. This ‘applicable crime’ purpose has two interpretations. First, it relates to preventing or detecting serious crime where authorities seek access to events data. This ‘serious crime’ term found in this purpose covers offences for which an adult can be sentenced to twelve months or more in prison.⁵⁵ The background behind introducing this ‘serious crime’ definition is interesting for tracking the reactionary changes to the IPA following *Tele2*.

Post-*Tele2*, the government proposed to lower the serious crime threshold for access to communications data to six months, but, following criticisms over broadening the scope of serious crime where only summary offences (e.g., usually minor offences that are tried in a magistrates’ court such as road traffic offences or common law assault) are excluded from the definition,⁵⁶ it set twelve-month imprisonment as the minimum threshold instead. However, this definition is a *second* crime threshold for serious crime because there is another statutory definition of serious crime in s. 263 of the IPA. Pre-*Tele2*, serious crime had already been defined under this section in the original version of the Act as (i) conduct involving the use of violence that results in substantial financial gain or by a large number of persons in pursuit of a common purpose; or (ii) an offence for which an adult could reasonably be expected to be sentenced to three years or more in prison. During the consultation process for the proposals to amend the IPA post-*Tele2*, including a separate ‘serious crime’ definition for authorisations of obtaining events data was criticised for making already complex legislation even more confusing.⁵⁷

The second interpretation of the ‘applicable crime’ purpose relates to preventing or detecting *crime* or preventing *disorder* where authorities seek access to communications data other than events data. The government introduced this bilateral ‘applicable crime’ purpose to impose a serious crime threshold for the acquisition and retention of events data while maintaining a lower crime threshold for the acquisition and retention of entity data based on its position that entity data encompasses subscriber data and is not covered by the CJEU’s *Tele2* decision. This interpretation of the *Tele2* decision, particularly in relation to the scope of data that it covered, was criticised by those who had argued that the CJEU did not differentiate the purposes for which different categories of communications data may be accessed in *Tele2*.⁵⁸ However, the CJEU’s later decisions in *Ministerio Fiscal*⁵⁹ and, more particularly, *Privacy International*⁶⁰ and *La Quadrature du Net*⁶¹ indicated the Court’s more nuanced approach to the different types of communications data because in the last of these decisions, the Court permitted indiscriminate retention of IP addresses for purposes related to the national security interest and serious crime, and ‘civil identity of subscribers’ (which may fall within the category of entity data under the IPA) for purposes related to ordinary crimes and public safety.⁶²

⁵⁵ IPA, s. 86(2A).

⁵⁶ Home Office, ‘Investigatory Powers Act 2016’, pp. 14–16.

⁵⁷ Big Brother Watch, ‘Big Brother Watch’s Response’; Liberty, ‘Liberty’s Response’. On this point, White notices the potential for the IPA falling short of the foreseeability requirements under the ECHR as part of the justification test for any Article 8 interference. See Matthew White, ‘Data Retention: Serious Crime or a Serious Problem’ (2019) 4 *Public Law* 633–643, 638.

⁵⁸ Big Brother Watch, ‘Big Brother Watch’s Response’; Liberty, ‘Liberty’s Response’. See also White, ‘Data Retention’, 639.

⁵⁹ *Ministerio Fiscal*.

⁶⁰ *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and others*.

⁶¹ *La Quadrature du Net and Others v. Premier Ministre and others*.

⁶² For commentary on the CJEU’s latest approach to data retention, see Marcin Rojszczak, ‘National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts’ (2021) 17(4) *European Constitutional Law Review* 607; Maria Tzanou and Spyridoula Karyda, ‘Privacy International and Quadrature du

As regards obtaining access to communications data for national security purposes, the Communications Data Code of Practice clarifies that the decision of whether an OCDA officer or a DSO of a public authority should grant the relevant authorisations is a matter for individual public authorities.⁶³ In this context, public authorities listed in Schedule 4 must have clear guidance in place about the authorisation route by a DSO for national security purposes ‘to allow OCDA to take informed decisions about resources required to maintain a good service’.⁶⁴ Finally, a DSO may authorise obtaining communications data when there is an urgent need to acquire the data because of an imminent threat to life or another emergency.⁶⁵

20.3.2.1.3 INTERNET CONNECTION RECORDS. Section 20.3.2.1.2 touched upon the differential treatment between events and entity data by imposing a serious crime threshold only for providing access to the former. The IPA also provides different standards for another sub-category of communications data. This sub-category is ICR, the scope of which is discussed in Section 20.2.1. Accordingly, a DSO may authorise obtaining of ICR if one of the three conditions are met.⁶⁶ The first condition is that access to the required ICR is necessary for one of the statutory purposes that can be found across s. 60A (on the prior authorisation by the OCDA), s. 61 (on the DSO authorisation) and s. 61A (on DSO authorisation in urgent cases). In essence, these purposes include the protection of national security interests, the protection of public safety interests, the ‘applicable crime’ purpose and the purpose of preventing death or injury. Access to ICR may be authorised based on any of these purposes to identify which person or apparatus is using an internet service where the internet service and the time of use are already known, but the identity of the person or apparatus is unknown.⁶⁷

The second condition according to which access to ICR may be authorised is that the data to be obtained falls within any of the statutory purposes mentioned just now other than those to prevent or detect serious crime or crime.⁶⁸ In other words, access to ICR may be authorised for non-crime-related purposes.⁶⁹ In this context, the data must be necessary to identify either of the following investigative purposes: (i) which internet communication service is being used, and when and how it is being used, by a person or an apparatus whose identity is known; (ii) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, a material whose possession is a crime; or (iii) which internet service is being used, and when and how it is being used, by a person or apparatus whose identity is already known.⁷⁰

As regards the third condition according to which ICR may be accessed, the IPA seems to incorporate both definitions of serious crime included in the Act.⁷¹ The original version of the Act, when it was first enacted, required access to ICR to pursue prevention and detection of

Net: One Step Forward Two Steps Back in the Data Retention Saga?’ (2022) 28(1) *European Public Law* 123; Valsamis Mitsilegas, Elspeth Guild, Elif Kuskonmaz and Niovi Vavoula, ‘Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks’ (January–March 2023) 29(1–2) *European Law Journal* 176–211, <https://doi.org/10.1111/eulj.12417>.

⁶³ Home Office, *Communications Data Code of Practice*, para. 5.19, p. 36.

⁶⁴ Ibid.

⁶⁵ IPA, s. 61A.

⁶⁶ IPA, s. 62(2).

⁶⁷ IPA, s. 62(3).

⁶⁸ IPA, s. 62(4).

⁶⁹ On this point, White questions the incompatibility of the IPA with the *Telez* and ECHR requirements. See White, ‘Data Retention’, 640.

⁷⁰ IPA, s. 62(4).

⁷¹ IPA, s. 62(5).

‘serious crime and other relevant crime’, the latter of which was defined as offences capable of incurring twelve months’ imprisonment per the original s. 62(6) of the IPA. This meant that ICR may be accessed for offences with a lower threshold. Following the public consultation for the proposed amendments post-*Tele2*,⁷² the government changed this section to exclude the notion of ‘other relevant crime’ from the purpose for which ICR may be accessed.

Following the 2018 amendments, to authorise access to ICR, the data to be obtained must be for the prevention or detection of the second type of serious crime that incurs twelve months’ imprisonment, or the data to be obtained must be for the prevention or detection of a crime but the crime to be prevented must be the first type of serious crime that incurs three years’ imprisonment. The second purpose is the same as the purpose required per the original s. 62(6) of the IPA. As for the first purpose, there is no substantive change except that the previous notion of ‘other relevant crime’ is covered by the second type of serious crime. Thus, despite the changes in the wording, lowering the threshold for serious crime with the introduction of a new definition also has an impact on lowering the thresholds for access to this specific sub-category of communications data. Finally, if either of these purposes is met, the data must be necessary for the investigatory purposes mentioned earlier on the second condition.⁷³

20.3.2.1.4 SINGLE POINTS OF CONTACT. The IPA gives statutory recognition to the role of SPoC as a communication channel between telecommunications operators and LEAs to ensure coordination between them.⁷⁴ According to the Act, SPoCs are accredited individuals or groups of individuals within, or related to, public authorities, who are trained to facilitate the lawful acquisition of communications data.⁷⁵ They are to be consulted by DSOs except in certain circumstances, such as where there is an imminent threat to life or another emergency or where there are national security interests.⁷⁶ The role of the SPoC is to advise DSOs on the most appropriate methods for obtaining the data concerned, the cost of and the resources for the requested access, as well as any unintended consequences and any issues as to the unlawfulness of the access authorisation.⁷⁷

20.3.2.2 Data Retention

Part 4 of the IPA sets out the rules for requiring telecommunications operators to retain communications data. At the centre lies the power of the Secretary of State to issue data retention notices.⁷⁸ To issue a data retention notice, the Secretary of State must consider whether retention is necessary for one or more of the statutory purposes, including national security interests, the ‘applicable crime’ purpose and being in the interests of public safety insofar as it is also relevant for the interests of national security.⁷⁹

In terms of the retention period, the maximum period for which the Secretary of State may issue a notice is twelve months from generation. There are no specific criteria for determining the length of the period, but the Secretary of State should consider the following elements before issuing a notice: the likely benefits of the notice, the likely number of users and the

⁷² Big Brother Watch, ‘Big Brother Watch’s Response’; Liberty, ‘Liberty’s Response’.

⁷³ IPA, s. 62(5).

⁷⁴ Under the Regulation of Investigatory Powers Act 2000 (RIPA), the role was merely standard practice.

⁷⁵ IPA, s. 76.

⁷⁶ Ibid.

⁷⁷ IPA, s. 76(5).

⁷⁸ IPA, s. 87(1).

⁷⁹ Ibid.

appropriateness of limiting the data to be retained by reference to location or descriptions of people to whom telecommunications services are provided.⁸⁰

Retention notices should contain certain elements.⁸¹ They may require retention of *all* data or any description of data by a particular telecommunications operator or *any* description of operators for a period of time.⁸² Even though the Secretary of State may tailor the notices accordingly, scholars have questioned the potential for retaining all communications data and the extent to which this may lead to vast data retention notices in scope.⁸³

20.4 DOMESTIC COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

20.4.1 Introduction

Under UK law, cooperation between service providers and LEAs in gathering information in the context of criminal investigations can be done on either a mandatory or a voluntary basis. There are different legal bases under which both types of cooperation can take place. Section 20.3 explored the legal basis for the two types of cooperation duties that are the most crucial: data acquisition and data retention regimes under the IPA. There are also other UK statutes (i.e., the Police and Criminal Evidence Act 1984 (PACE), the Police Act 1997, the Terrorism Act 2000, and the Proceeds of Crime Act 2002) that confer powers on LEAs for specific coercive and covert investigatory measures that may oblige service providers to cooperate with them in the context of criminal investigations. An overview of these statutes is provided in Section 20.4.3.4.

The annual reports of the IPC indicate how often LEAs resort to cooperation with (national) service providers. According to the 2020 report, a total of 331,111 applications were submitted by LEAs and the police seeking acquisition of communications data for the period 1 January to 31 December 2020.⁸⁴ Of all these applications, 239,086 were authorised by the OCDA.⁸⁵ The majority of those authorisations (81,800) were acquired for drug offences.⁸⁶ The second highest number of authorisations (36,668) were acquired for ‘other offences’, which the IPC does not define in the report.⁸⁷ This was followed by authorisations related to sexual offences, with a total number of 30,675 authorisations.⁸⁸

Moreover, in his report on the investigatory powers of LEAs (and intelligence authorities) under the regime preceding the IPA, the Independent Reviewer of Terrorism Legislation indicated the high reliance of LEAs on interception of content communications (2,795 warrants were issued in 2014) and acquisition of communications data (investigation of 90 per cent of all

⁸⁰ IPA, s. 88(1).

⁸¹ IPA, s. 87.

⁸² IPA, s. 87(2).

⁸³ See McKay, ‘Blackstone’s Guide’, para. 5.07, p. 105. See also Andrew Murray, ‘Data Transfers between the EU and UK Post Brexit?’ (2017) 7(3) *International Data Privacy Law* 149, 161 [the author agrees that the language of the IPA in setting out what elements a data retention notice must contain is susceptible to imposing ‘generalised and indiscriminate’ notice]; Jennifer Cobbe, ‘Casting the Dragnet: Communications Data Retention under the Investigatory Powers Act’ (2018) *Public Law* 10, 15 [the author considers the potential for a data retention notice to require the retention of all data irrespective of a link between the data and the threat to public security].

⁸⁴ IPCO and OCDA, *Annual Report*, 104.

⁸⁵ *Ibid.*, 94.

⁸⁶ *Ibid.*, 95.

⁸⁷ *Ibid.*

⁸⁸ *Ibid.*

serious crimes).⁸⁹ According to this report⁹⁰, LEAs have relied more on their powers to obtain communications data, instead of on those other evidential powers, such as search and seizure, conferred on them.⁹¹ This was because the LEAs claimed that the

[u]se of communications data can build a case for using a more intrusive measure, or deliver the information that makes other measures unnecessary. It can, and does, exonerate innocent people without them needing to know that they were ever under suspicion. Its marginal cost is low; it can be started, changed and stopped easily; it involves a low risk of compromising an investigation by being discovered by the suspects[;] and it is able to be used much more widely than other forms of surveillance.⁹²

Along with the mandatory cooperation duties for service providers, UK law provides voluntary cooperation mechanisms according to which they can share information with LEAs in the context of criminal investigations. The statutory provisions that yield such voluntary cooperation do not provide a procedure for that cooperation. Instead, they exempt service providers from liabilities that may otherwise have arisen because of the disclosure of information (e.g., non-compliance with the data protection principles).⁹³

The 2015 report of the Independent Reviewer of Terrorism Legislation highlighted that voluntary cooperation had been taking place, but without providing more precise data.⁹⁴ Although the report dates to the legislation before the IPA, it shows the concerns that the UK-based service providers had over this voluntary cooperation. Those concerns relate to the lacks of judicial oversight, accountability and transparency, as well as the patchwork of LEA powers scattered across laws, and the cost of cooperation.⁹⁵ Indeed, the same report showed that service providers would prefer suitably circumscribed and human rights-respecting statutory obligations as opposed to voluntary arrangements because, in this way, they would be able to maintain their customers' trust while complying with those obligations.⁹⁶ Following enactment of the IPA, LEAs are expressly prevented from relying on voluntary cooperation mechanisms where the data may be obtained by the investigatory powers under the IPA.⁹⁷

20.4.2 *Nature of the Cooperation*

As mentioned in Section 20.4.1, cooperation between LEAs and service providers takes place on both a mandatory and a voluntary basis. Information obtained through both types of cooperation can be used as evidence before UK courts.⁹⁸ Rules and laws that apply to that information are the

⁸⁹ David Anderson QC, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015), paras 7.14 and 7.47, pp. 127 and 135, <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf>.

⁹⁰ This report provides a general overview of the then surveillance powers of LEAs and makes recommendations for reform of those powers in the post-IPA era to provide safeguards to individuals.

⁹¹ Anderson, *A Question of Trust*, para. 9.30, p. 172.

⁹² *Ibid.*

⁹³ Section 20.4.3 in this chapter.

⁹⁴ Anderson, *A Question of Trust*, para. 11.29, pp. 209–210.

⁹⁵ *Ibid.*

⁹⁶ *Ibid.*, para. 11.7, p. 204.

⁹⁷ Home Office, *Communications Data Code of Practice*, para. 1.5, p. 5 ['Relevant public authorities should also not require, or invite, any postal or telecommunications operator to disclose communications data by relying on any exemption to restrictions on disclosing personal data under relevant data protection legislation'].

⁹⁸ The exceptional circumstances where the content of communications obtained through interception can be admissible evidence are discussed in Section 20.4.3.1 of this chapter.

same as those that apply to documentary evidence.⁹⁹ That information can be disclosed provided it is not the subject of an application for a public interest immunity certificate, details of which are discussed in Section 20.4.4. Courts also have the discretion to exclude evidence which may otherwise endanger the fairness of the trial.¹⁰⁰ Thus, a defendant can request the exclusion of evidence on the grounds of either the procedure through which evidence was obtained or its reliability. Third parties, such as service providers, cannot challenge the evidence but can be heard as witnesses.

As for the enforceability of the mandatory duties, those duties under the IPA are enforceable by civil proceedings. Section 20.3 discussed two of these duties: acquisition of communications data¹⁰¹ and retention of communications data.¹⁰² Section 20.4.3 will provide an account of the other mandatory duties (i.e., interception,¹⁰³ equipment interference¹⁰⁴ and technical capability notices¹⁰⁵) for which the Secretary of State preserves the power to start civil proceedings for an injunction or specific performance about a slow or late reply by the service provider. However, to date, the Secretary of State has chosen not to pursue enforcement actions against service providers partly because they would not want to experience the associated publicity. Instead, there has been a culture of negotiating a mutually acceptable arrangement.

In addition to civil proceedings, the IPA sets out an offence for failing to comply with the duties in relation to interception. It is thus an offence to knowingly fail to comply with the obligation to give effect to an interception warrant, which is punishable by a maximum twelve months' imprisonment, a fine or both in England and Wales on summary conviction.¹⁰⁶ On conviction on indictment, the offence is punishable by a maximum two years' imprisonment, a fine or both.¹⁰⁷

However, telecommunications operators can raise the defence that they are not required to take steps (e.g., technical, organisational or financial) in pursuance of warrants, orders or authorisations under the IPA that are not *reasonably practicable* to take to justify their non-compliance.¹⁰⁸ This reasonableness standard is objective and does not depend on what the service operators think is reasonable in their view. Particularly with regard to data retention notices, the IPA allows telecommunications providers to refer the notice to the Secretary of State for revision.¹⁰⁹ The period within which the referral can be made and the circumstances for which it can be made will be addressed under regulations that have not yet been drafted. The Secretary of State then consults the Technical Advisory Board, which considers the technical and financial consequences of the respective data retention notice, and a Judicial Commissioner (JC), which considers the proportionality of that notice.¹¹⁰ After receiving the conclusions made by these bodies, the Secretary of State can withdraw or modify the notice or give further notice.¹¹¹ It can only modify the first notice or give further notice upon the approval of the IPC.¹¹²

⁹⁹ Section 20.3.1 of this chapter.

¹⁰⁰ PACE, s. 78.

¹⁰¹ IPA, s. 66.

¹⁰² IPA, s. 95.

¹⁰³ IPA, s. 43.

¹⁰⁴ IPA, s. 128.

¹⁰⁵ IPA, s. 255.

¹⁰⁶ IPA, s. 43(7)(a).

¹⁰⁷ IPA, s. 43(7)(d).

¹⁰⁸ IPA, ss. 43(3), 66(3), 128(5). See Section 20.5.2.3 of this chapter for discussion on the conflict of laws defence.

¹⁰⁹ IPA, s. 90. This provision will be amended by the Investigatory Powers (Amendment) Act 2024.

¹¹⁰ IPA, s. 90(6)–(8).

¹¹¹ IPA, s. 90(10).

¹¹² IPA, s. 90(11).

In relation to the other mandatory duties prescribed in UK law, neither of the statutes explored in Section 20.4.3.4 explicitly addresses situations that would be considered a refusal to cooperate. However, they impose statutory deadlines, and failing to meet them would be considered a refusal, raising potential criminal liabilities for contempt of court. For example, under PACE, a person in possession of the requested material shall produce it to a constable or give a constable access to it not later than at the end of the period of seven days from the date of the order or at the end of a longer period that the order may specify.¹¹³ If the person subjected to an order issued under PACE Schedule 1 fails to comply with it within the specified time, the judge may deal with that person for contempt of court, which is punishable by a fine or a maximum of two years imprisonment. In terms of the liability of the service provider for contempt of court, the representative of that provider or the individual targeted in the production order may be found liable.

As opposed to the mandatory cooperation duties, the voluntary cooperation of service providers depends on their willingness to cooperate with LEAs. However, as mentioned earlier, LEAs should not circumvent the mandatory route of obtaining information from telecommunications operators under the IPA, and thus, they should not use a voluntary route if they can obtain the requested information under the IPA.¹¹⁴ In particular, DPA 2018 exempts controllers from the obligations under the general principles and other provisions where compliance would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.¹¹⁵ However, voluntary disclosure by telecommunications operators based on this exemption should be rare in cases where the disclosed information could have been obtained by the investigatory powers under the IPA. In his 2020 annual report, the IPC noted this ‘IPA v. DPA’ problem.¹¹⁶ The IPC provides the following example in explaining the problem:

The most common problem arises where a telecommunications operator determines material is communications data ... and insists on an authorisation under the IPA to disclose that information to the LEA. The LEA submits an application to OCDA to acquire the data, but OCDA refuses the application because it does not consider the material being sought to fall under the IPA definition of communications data.¹¹⁷

The IPC noted that ‘the complexity and ambiguity of the definition continues to pose very real difficulties for public authorities and telecommunications operators’.¹¹⁸

20.4.3 Overview of Existing Cooperation Duties

As mentioned in Section 20.4.1, the IPA imposes mandatory cooperation duties on service providers in addition to those duties relating to data retention and acquisition. Under the IPA, there are cooperation duties with respect to interception, equipment interference and technical capability notices. Information obtained through these procedures may be used for intelligence or evidential purposes, except content obtained through interception which is inadmissible in any legal proceedings and is therefore for intelligence purposes only.¹¹⁹

¹¹³ PACE, Sch. 4.

¹¹⁴ Home Office, *Communications Data Code of Practice*, para. 1.5, p. 5.

¹¹⁵ DPA 2018, s. 15 and Sch. 2, Pt 1, para. 2.

¹¹⁶ IPCO and OCDA, *Annual Report*, 90.

¹¹⁷ *Ibid.*

¹¹⁸ *Ibid.*

¹¹⁹ IPA, s. 56.

Several other statutes provide investigatory powers to LEAs in terms of obtaining information for the prevention and detection of crime-related purposes. This subsection provides a summary of each of these additional duties in turn. Voluntary cooperation is excluded for these measures because, as mentioned earlier, the respective statutory bases for that cooperation do not set out a procedure according to which service providers may share information with LEAs.

20.4.3.1 Interception

According to the IPA,

a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if (a) the person does a relevant act in relation to the system, and (b) the effect of the relevant act is to make any content of the communication available, *at a relevant time*, to a person who is not the sender or intended recipient of the communication.¹²⁰

The relevant time for an interception to occur is ‘(a) any time while the communication is *being transmitted*, and (b) any time when the communication is *stored in or by the system* (whether before or after its transmission)’.¹²¹ The condition of whether the communication is intercepted while being transmitted or while being stored by the system is a crucial one because the intercepted material obtained while the communication is ‘being transmitted’ is not admissible as evidence in legal proceedings, although it might have been lawfully obtained.¹²² There are a few exceptions to this rule, one being where the interception of communication was *lawful by equipment interference warrant* when the communication is *stored in or by a telecommunication system*.¹²³

This means that if the intercepted material is obtained while ‘being transmitted’, an interception warrant is required to obtain it lawfully. If the intercepted material is obtained while ‘being stored in or by a telecommunication system’, an equipment interference warrant is required to obtain it lawfully. Otherwise, interception without an appropriate warrant issued by an appropriate authority is recognised as a criminal offence.¹²⁴ However, there are slight differences between the requirements for which an interception warrant and an equipment interference warrant may be issued. The authorities who have the power to apply for an interception warrant differ from the authorities who may issue an equipment interference warrant because, for the latter, LEAs may also issue an equipment interference warrant in addition to the Secretary of State on certain grounds.¹²⁵ Those grounds for which they may issue an equipment interference warrant are different from those for which an interception warrant may be issued because the former involves purposes other than national security interests or the prevention and investigation of serious crime.

On the other hand, the Secretary of State has the exclusive power to issue an interception warrant upon application by heads of several intelligence and security agencies (i.e., the heads of the intelligence services MI5, MI6 and GCHQ, the National Crime Agency (NCA), the Metropolitan Police, the Police Services of Scotland and Northern Ireland, HM Revenue and

¹²⁰ IPA, s. 4(1) [emphasis added].

¹²¹ IPA, s. 4(4) [emphasis added].

¹²² IPA, s. 56.

¹²³ IPA, Sch. 3(2)(1)(a) [emphasis added].

¹²⁴ IPA, s. 3.

¹²⁵ Section 20.4.3.2 of this chapter.

Customs, the Chief of Defence Intelligence).¹²⁶ The Secretary of State may issue a warrant if he or she believes that it is necessary on certain grounds and proportionate to what is sought.¹²⁷ The grounds are national security; preventing or detecting serious crime; safeguarding the economic well-being of the UK, insofar as that is relevant to national security; or giving effect to an international mutual assistance agreement.¹²⁸ This decision by the Secretary of State is then subject to approval by a JC.¹²⁹

The difference between the communications ‘being transmitted’ and ‘being stored in or by a telecommunication system’ was considered in *R v. A, B, D & C*.¹³⁰ The case related to the use of intercepted messages obtained by the NCA from the Encrochat messaging service, which provided anonymity for its users and which, as later revealed, was infiltrated by the French police using malware, which affected the devices in the UK. The NCA obtained the evidence after issuing a European Investigation Order (EIO) to the French police.¹³¹ The appellants argued that the material obtained through the messaging service was still in transit at the time it was taken by the NCA, and it was inadmissible in criminal proceedings. For this reason, the appellants argued that the messages were unlawfully obtained by equipment interception warrant when they should have been obtained by interception warrant.¹³² The Court of Appeal, however, rejected this main argument by the appellants. First, it held that the statutory provision in relation to the relevant time when the interception occurs (i.e., in transmission or storage) must work irrespective of the technical features of the system in question.¹³³ The court further compared the provision with the rules relating to interception under the pre-IPA legislation that limited the meaning of ‘storage’ to where the intended recipient accesses the communication,¹³⁴ which under the old regime indicated that the communication was being transmitted unless it was accessed by the recipient.¹³⁵

The IPA does not contain any such limitation to the meaning of ‘storage’ and thus the notion of communication ‘being stored’ could encompass all forms of storage regardless of whether they are accessed by the recipient.¹³⁶ Thus, the wording of the provision which includes the word ‘and’ instead of ‘or’ suggested that the conditions for communications being in transit and being stored in a telecommunications service were not mutually exclusive.¹³⁷ This meant that whether the communication was stored before or after its transmission was irrelevant. The only distinction was the appropriate warrant required to obtain communications and whether the material would be admissible in legal proceedings.¹³⁸ In any case, the malware took the messages from the devices before they were being encrypted on the sending device and after decryption on the receiving device and, they were copied from the data held on the sending and receiving devices.¹³⁹ Thus, the

¹²⁶ IPA, ss. 18–19.

¹²⁷ IPA, s. 19.

¹²⁸ IPA, s. 20.

¹²⁹ IPA, s. 23.

¹³⁰ *R v. A, B, D & C* (see footnote 3).

¹³¹ The EIO order was subject to judicial review request, but this request was unsuccessful. See *R (C) v. Director of Public Prosecutions* [2020] EWHC 2967 Admin.

¹³² *R v. A, B, D & C*, para. 15.

¹³³ *R v. A, B, D & C*, para. 55.

¹³⁴ *R v. A, B, D & C*, para. 59.

¹³⁵ *Edmondson & ors v. R* [2013] EWCA Crim 1026.

¹³⁶ *R v. A, B, D & C*, para. 59.

¹³⁷ *R v. A, B, D & C*, para. 61.

¹³⁸ *Ibid.*

¹³⁹ *R v. A, B, D & C*, para. 66.

communication was obtained when being stored based on an equipment interception warrant and, therefore, was admissible in criminal proceedings.

In addition to this issue of when the interception occurs, another question is who the ‘lawful authority’ is in respect of an interception. This question was particularly prevalent under the legislation preceding the IPA, the Regulation of Investigatory Powers Act 2000 (RIPA). The meaning of lawful authority for interception under RIPA was raised in *R (NTL Group Limited) v. Ipswich Crown Court*.¹⁴⁰ The communications company NTL sought judicial review of a court order issued under section 9 and Schedule 1 of PACE, which is mentioned in Section 20.4.3.4. The company argued that to comply with the order, it would have to copy the unopened emails to an email address different from the intended recipient’s because of how its email system operated. Only after this transmission could the police have access to the emails. The transmission meant that they would intercept the content of communications. However, no interception warrant was issued for this interception. Without the warrant, they would not have the lawful authority to carry out the interception and would effectively commit an interception offence under RIPA. The Court of Appeal dismissed this claim and held that the police had lawful authority to request NTL to execute an order under PACE.¹⁴¹ To reflect this *NTL* decision,¹⁴² the IPA includes two circumstances (in addition to interception in accordance with the equipment interference warrant discussed in Section 20.4.3.1 in the *R v. A, B, D & C* decision) in determining the lawful authority for interception of ‘stored’ communication.¹⁴³ First, the interception is carried out in the exercise of any statutory power to obtain information or take possession of any document or other property.¹⁴⁴ Second, it is carried out in accordance with a court order made for that purpose.¹⁴⁵

20.4.3.2 Equipment Interference

Part 5 of the IPA sets out the rules for the use of equipment interference techniques by LEAs, security and intelligence agencies. Colloquially known as ‘hacking’, these techniques had been used by agencies under sections 5 and 7 of the Intelligence Services Act 1994 before the IPA was enacted, and only in 2015 did the UK government publicly admit to their use following a legal challenge against these techniques.¹⁴⁶ Despite the introduction of the IPA, these provisions remain in operation, but they are available only for authorising interference with equipment, and not to acquire communications data.¹⁴⁷ If authorisation for equipment interference is sought to obtain communications data, the appropriate legal basis is the IPA.¹⁴⁸

The scope of equipment interference under the IPA, however, is broader than obtaining communications data. It may include ‘communications’ (e.g., speech, music, sound, visual

¹⁴⁰ *R (NTL Group Limited) v. Ipswich Crown Court* [2002] EWHC 1585 (Admin), [2003] EWCA Cr App R 14.

¹⁴¹ *R (NTL Group Limited) v. Ipswich Crown Court*, para. 23.

¹⁴² McKay, ‘Blackstone’s Guide’, para. 2.42, p. 37.

¹⁴³ The IPA defines ‘lawful authority’ for the first time in its s. 6.

¹⁴⁴ IPA, s. 6(1)(c)(ii).

¹⁴⁵ IPA, s. 6(1)(c)(iii).

¹⁴⁶ *Privacy International and Greennet and Others v. (1) The Secretary of State for Foreign and Commonwealth Affairs (2) The Government Communications Headquarters*, IPT14/85/CH14/120–126/CH. See also Nora Ni Loideain, ‘A Bridge Too Far? The Investigatory Powers Act 2016 and Human Rights Law’, in Lilian Edwards (ed.), *Law, Policy and the Internet* (Oxford: Bloomsbury, 2018), 165–192, 180–181.

¹⁴⁷ Home Office, *Equipment Interference Code of Practice* (March 2018), para. 3.37, p. 19, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf.

¹⁴⁸ Home Office, *Equipment Interference Code of Practice*, para. 3.37, p. 19.

images or data, and signals between a person and a thing or between things), ‘equipment data’¹⁴⁹ (e.g., messages sent between items of network infrastructure, account identifiers such as email address or user identifier (ID), or data that may be used to identify any person, apparatus, system, event or the location of any person, event or thing¹⁵⁰) and ‘other information’.¹⁵¹ This broad scope of equipment interference thus covers downloading data from a device (mobile phones, computer laptops or Internet of Things (IoT) devices) or using keylogging software to monitor the user of the device.¹⁵²

The head of the security and intelligence services (e.g., GCHQ, MI5, MI6, Defence Intelligence) may apply to the Secretary of State to issue a warrant to authorise equipment interference in the interests of national security, to prevent or detect serious crime¹⁵³ or in the interests of the economic well-being of the country insofar as these interests are relevant to the interest of national security.¹⁵⁴ An equipment interference warrant issued by the Secretary of State must be approved by a JC.¹⁵⁵

The IPA also provides powers to issue equipment interference warrants to the heads of specified LEAs (e.g., the Metropolitan Police).¹⁵⁶ This means that, unlike the procedure whereby the heads of the intelligence and security agencies may apply for an equipment interference warrant, the Secretary of State does not issue the warrant. Nevertheless, a warrant issued by the heads of the specified LEAs must be approved by a JC.¹⁵⁷ The heads of the specified LEAs have the power to issue an equipment interference warrant to prevent and detect serious crime or to prevent death, injury or damage to a person’s physical or mental health or to mitigate injury or damage to physical or mental health.¹⁵⁸

The use of equipment interference techniques by the intelligence and security agencies and LEAs may trigger application of the Computer Misuse Act (CMA) 1990 where their conduct amounts to computer offences prescribed by the Act.¹⁵⁹ However, where an equipment interference warrant is issued according to the IPA, the conduct will be deemed to be ‘authorised’, and no offence under the CMA 1990 will be committed.¹⁶⁰

In terms of how often the relevant authorities resort to equipment interference techniques, in his 2020 annual report, the IPC recorded that a total of 1,306 equipment interference authorisations were granted for LEAs and a total of 1,915 equipment interference authorisations were granted for intelligence and security agencies.¹⁶¹ There was thus a slight increase in the number of authorisations granted for LEAs and the relevant agencies because in 2019 a total of 848 authorisations were granted for the former, while a total of 1,071 authorisations were granted for the latter.¹⁶²

¹⁴⁹ IPA, ss. 100 and 107.

¹⁵⁰ Home Office, *Equipment Interference Code of Practice*, paras. 2.3–2.5, pp. 6–8.

¹⁵¹ IPA, s. 99(2).

¹⁵² Home Office, *Equipment Interference Code of Practice*, para. 3.3, p. 10.

¹⁵³ Which requires a minimum of three years’ imprisonment (IPA, s. 263(1)).

¹⁵⁴ IPA, s. 102(5).

¹⁵⁵ IPA, s. 102(1)(d).

¹⁵⁶ IPA, s. 106. Schedule 6 provides a list of LEAs and their designated chief officers who have the power to issue an equipment interference.

¹⁵⁷ IPA, s. 106(1)(d).

¹⁵⁸ IPA, s. 106(1)–(3).

¹⁵⁹ Computer Misuse Act (CMA) 1990, ss. 1–3A.

¹⁶⁰ Home Office, *Equipment Interference Code of Practice*, paras. 3.6–3.9, p. 11. See also CMA 1990, s. 10.

¹⁶¹ IPCO and OCDA, *Annual Report*, 139.

¹⁶² *Ibid.*

20.4.3.3 Technical Capability Notices

The authority to issue a technical capability notice rests with the Secretary of State,¹⁶³ but the IPA requires him or her to consult the telecommunications operator who may be the subject of the notice before issuing one.¹⁶⁴ The notice must also be approved by a JC.¹⁶⁵

The notice may impose several *ex ante* obligations on telecommunications operators, requesting them to put in place the capability to respond to future interception warrants, data acquisition authorisations, data retention notices and equipment interference warrants.¹⁶⁶ One obligation has been the subject of debate: '[t]o provide and maintain the capability to disclose, where practicable, the content of communications or secondary data in an intelligible form *and to remove electronic protection* applied by or on behalf of the telecommunications operator to the communications or data, or to permit the person to whom the warrant is addressed to remove such electronic protection'.¹⁶⁷ When the IPA was first enacted, critics viewed this obligation as a way to impose an obligation on telecommunications operators to remove end-to-end encryption.¹⁶⁸ It is now generally agreed that this obligation would not enable LEAs to request the removal of end-to-end encryption once implemented since the encryption is applied by the device, not the service provider. However, a technical capability notice could be used to prevent the implementation of end-to-end encryption by the service provider in the first place. At the time of writing this chapter, there is no publicly available information about how many technical capability notices have been issued under the IPA.

20.4.3.4 Other Investigatory Powers in Obtaining Data

As mentioned earlier, several statutes provide investigatory powers to LEAs and, in the exercise of these powers, service operators have mandatory duties to cooperate. First of all, PACE grants the police rights to access and remove files from computers on site to obtain 'excluded material' (i.e., personal records created in the course of any trade, business or other occupation which is held subject to a duty of confidence, medical records or journalistic material) and 'special procedure material' (i.e., a material other than items subject to legal privilege and excluded material in the possession of who acquired them in the course of any trade, business or other occupation which is held subject to a duty of confidence, and journalistic material other than that which falls within the scope of excluded material).¹⁶⁹ To obtain the relevant material, the police must have a search order issued by a circuit judge.¹⁷⁰

Second, the Police Act 1997 covers the statutory power of the police to interfere with private property, including the use of surveillance devices.¹⁷¹ The Act designates the officer who has the power to authorise interference with private property within each competent public authority (including police forces, transport police, the director of the National Criminal Intelligence

¹⁶³ IPA, s. 253.

¹⁶⁴ IPA, ss. 253(1)(a)–(b) and 253(6).

¹⁶⁵ IPA, s. 253(1)(c).

¹⁶⁶ Investigatory Powers (Technical Capability) Regulations 2018/353 (Regulations 2018/353).

¹⁶⁷ Regulations 2018/353, Sch. 1, para. 8 [emphasis added].

¹⁶⁸ Asaf Lubin, 'UK Investigatory Powers Act and International Law: Part I', UCL Blog, 26 December 2016, <https://blogs.ucl.ac.uk/law-journal/2016/12/26/the-investigatory-powers-act-and-international-law-part-i/>; Privacy International, 'UK Investigatory Powers Bill Will Require Tech Companies to Notify the Government of New Products and Services in Advance of Their Launch', 11 April 2016, <https://privacyinternational.org/blog/1152/uk-investigatory-powers-bill-will-require-tech-companies-notify-government-new-products>.

¹⁶⁹ PACE, s. 9.

¹⁷⁰ PACE, Sch.1.

¹⁷¹ Police Act 1997, Part III.

Service) by rank.¹⁷² That officer may issue an authorisation if he or she believes it to be necessary and proportionate to prevent the commissioning of serious crime.¹⁷³ The authorisation must be approved by a JC to take effect.¹⁷⁴

Third, the Proceeds of Crime Act 2002 gives powers to the police to access information about investigations on money laundering by way of production orders.¹⁷⁵ A production order may be issued if there are reasonable grounds for suspecting that the person is subject to money laundering investigations.¹⁷⁶ This issuance may be done if there are reasonable grounds for believing that the person in question is in possession or control of the material requested.¹⁷⁷ There must also be reasonable grounds for believing that the material is likely to be of substantial value for the investigation and that it is in the public interest to produce the material or have access to it, taking into account its benefit for the terrorist investigation and the circumstances under which the person concerned appears to have the material in his or her possession or control.¹⁷⁸

Finally, the Terrorism Act 2000 covers the statutory power of ‘an appropriate officer’ (i.e., a constable or a counterterrorism financial investigator) to apply to a circuit judge to grant a production order to obtain information relating to a terrorist investigation.¹⁷⁹ The order may require a specified person to produce or to give access to a material which he or she has in his or her possession or control or may require that person to state to the best of his or her knowledge the location of the material if it is not in his or her possession.¹⁸⁰

20.4.4 *Legal Remedies and Protection of Fundamental Rights*

The Human Rights Act 1998 (HRA) incorporates the rights established in the European Convention on Human Rights (ECHR) into UK law. According to section 3 of the Act, all UK laws must be read and given effect, so far as it is possible to do so, in a way that is compatible with the rights set out in the Act. These rights include Articles 8 and 10 of the ECHR. Thus, it is unlawful for LEAs and intelligence and security agencies to act in a way that is incompatible with the rights set out in the ECHR. For claims relating to their powers under the IPA, the Investigatory Powers Tribunal (IPT) has exclusive jurisdiction.¹⁸¹ The applicant can make a claim before the IPT if there is a suspicion that he or she might be subjected to surveillance. Since the IPT was established in 2000 by RIPA 2000, there have been several challenges before the European Court of Human Rights (ECtHR) questioning its effectiveness as a judicial redress mechanism in light of the ECHR requirements. Since its *Kennedy* decision, the ECtHR has confirmed an effective remedial mechanism status to the IPT.¹⁸² However, under the old regime, the decisions of the IPT could not be subject to appeals. This changed with the IPA, which introduces an appeal procedure for the IPT’s decisions, whereby claimants can appeal against

¹⁷² Ibid., s. 97(5).

¹⁷³ Ibid., s. 93(2).

¹⁷⁴ Ibid., s. 97.

¹⁷⁵ Proceeds of Crime Act (PCA) 2002, s. 352.

¹⁷⁶ Ibid., s. 346(2).

¹⁷⁷ Ibid., s. 346(3).

¹⁷⁸ Ibid., ss. 346(4)–(5).

¹⁷⁹ Terrorism Act 2000, Sch. 5.

¹⁸⁰ Ibid., Sch. 5, para. 5.

¹⁸¹ IPA, ss. 242–243. For a discussion on the jurisdiction of the IPT, see Maria Helen Murphy, *Surveillance and the Law: Language, Power, and Privacy* (Abingdon: Routledge, 2019).

¹⁸² *Kennedy v. the UK*, Appl. No. 26839/05, 18 May 2010.

decisions and determinations by this Tribunal on a point of law to the Court of Appeal in England and Wales, the Court of Session or the Court of Appeal in Northern Ireland.¹⁸³

As regards the HRA claims for mandatory cooperation duties under PACE, the Terrorism Act 2000, the Police Act 1997 and the Proceeds of Crime Act, the UK courts have considered that a fair balance must be struck between disclosure of information and HRA rights (e.g., the right to privacy where the disclosure of information involves transfer and processing of personal information and freedom of expression where the disclosure of information concern journalistic material). For example, in *R (Malik) v. Manchester Crown Court*, the UK Court held that section 5 of the Terrorism Act 2000 ‘strike[s] a balance between the object of enabling the police to conduct terrorist investigations effectively and respect for a journalist’s article 10 rights. To the extent that there is a conflict between that object and respect for a journalist’s rights, the court is required to weigh the competing considerations and make a judgment.’¹⁸⁴

Moreover, judicial review is available as a safeguard against the use of investigatory powers under PACE, the Terrorism Act 2000, the Police Act 1997 and the Proceeds of Crime Act. This will involve reviewing the issuance of a search order (PACE), a production order (Terrorism Act 2000 or Proceeds of Crime Act 2002) or an authorisation (Police Act 1997) on the grounds of legality, rationality, procedural impropriety and proportionality (in cases involving human rights claims).¹⁸⁵ The decisions of the IPT are also open to judicial review if they involve an error of law, even though the IPA provides a statutory route for the appeal procedure.¹⁸⁶

The most polarising debate on fundamental rights protection against investigatory powers has been held about those powers prescribed by the IPA. As mentioned in Section 20.4.4, the IPA provides several safeguards the effectiveness of which have been subject to ongoing debates and legal challenges. In essence, these safeguards can be summarised into three points: (i) the introduction of the JCs, (ii) the protection afforded to privileged items and (iii) the requirement to notify individuals who have been affected by LEAs’ and intelligence and security agencies’ use of investigatory powers.

The role of the JCs is to review the notices, warrants and authorisations issued under the IPA except in cases of urgency. It was introduced by the IPA to meet with the ‘independent review’ mechanism highlighted by the CJEU in its *Digital Rights Ireland* and *Tele2* decisions, the latter of which was delivered as the Act was in its Bill stage.¹⁸⁷ The Prime Minister appoints JCs for a term of three years;¹⁸⁸ to be eligible for the position, an individual must hold or have held a high judicial office.¹⁸⁹ The government considered the JCs’ role a means to provide stronger oversight mechanisms.¹⁹⁰

¹⁸³ RIPA, s. 67A as amended by IPA, s. 242.

¹⁸⁴ *R (Malik) v. Manchester Crown Court* [2008] EWHC 1362, para. 55.

¹⁸⁵ *Council of Civil Service Unions v. Minister for the Civil Service* [1985] AC 374.

¹⁸⁶ *(Privacy International) v. Investigatory Powers Tribunal* [2019] UKSC 22. It is sufficient to note here that the legal dispute arose from an ‘ouster clause’, according to which statutory provision declares a tribunal or other body final and excludes the jurisdiction of courts or judicial review process, incorporated into the old regime by RIPA 2000. The Supreme Court overturned the High Court’s decision, which had held that the ouster clause sufficed to prevent it from carrying out judicial review against the IPT’s decisions. The Supreme Court’s decision on the reviewability of the IPT led to another judicial review request by the civil society organisation Liberty, for a range of powers prescribed by the IPA, including the data acquisition regime. The High Court delivered its opinion in July 2019 and held that the powers were not incompatible with the ECHR requirements. See *R (National Council for Civil Liberties) v. Secretary of State for the Home Department* [2019] EWHC 2057 (Admin).

¹⁸⁷ McKay, ‘Blackstone’s Guide’, paras 5.03–5.04, p. 104. See also Eleni Kosta, ‘The Retention of Communications Data in Europe and the UK’, in Lilian Edwards (ed.), *Law, Policy and the Internet* (Oxford: Bloomsbury, 2018), 193–212.

¹⁸⁸ IPA, ss. 227(1) and 228(2).

¹⁸⁹ IPA, s. 227(2).

¹⁹⁰ On discussions around the introduction of JCs, see Ni Loideain, ‘A Bridge Too Far?’, 187; Matthew White, ‘The Threat to the UK’s Independent and Impartial Surveillance Oversight Comes Not Just from the Outside, but from

There were concerns from scholars over the scope of the review of the JCs. According to the IPA, in reviewing a data retention notice, a JC must apply the principles of judicial review, which in essence determine the lawfulness of a decision or action made by a public authority.¹⁹¹ The absence of reference to the proportionality and the necessity of the notice was interpreted as a way in which the scope of the review powers of JCs was limited compared to the powers that would have required them to evaluate the necessity and the proportionality of the notice in their own right, instead of evaluating the conclusions of the Secretary of State.¹⁹² As a response, the IPC thus issued advisory guidance in March 2018 on the scope of their powers to approve data retention notices (as well as the other warrants as required by the IPA).¹⁹³ It clarified that '[t]he purpose of the so-called "double lock" provisions of the Act are to provide an independent, judicial, safeguard as to the legality of warrants, in particular to their necessity and proportionality'.¹⁹⁴

As regards the second safeguard, the IPA provides additional safeguards for privileged items (e.g., the content of communications sent by or intended to Members of Parliament, items subject to legal professional privilege, confidential journalistic material and sources of journalistic information) when they are obtained by the investigatory powers laid out therein. It thus recognises separate procedures for each power according to which the items can be obtained. Some of the investigatory powers (e.g., data acquisition powers) adduce additional safeguards to some of the subtypes of privileged items, but not all types of information. In essence, the safeguards involve approval by a JC (for authorisation to obtain communications data to identify or confirm journalistic information¹⁹⁵) or the Prime Minister (for issuing equipment interference warrants and interception warrants that might involve materials sent by or intended to Members of Parliament).¹⁹⁶ In other instances, the IPA requires additional factors to be considered before the issuance of a warrant.¹⁹⁷

However, in its *Big Brother Watch* decision, the Grand Chamber of the ECtHR affirmed that there must be a priori authorisation by the judiciary or an independent and impartial body that must review the potential risks and benefits of obtaining journalistic material by way of using investigatory powers, to comply with the requirements under Article 10 of the ECHR that

Within' (2019) 5 *European Human Rights Law Review* 512; Paul F. Scott, 'Hybrid Institutions in the National Security Constitution: The Case of the Commissioners' (2019) 39(3) *Legal Studies* 432.

¹⁹¹ IPA, s. 89(2)(a).

¹⁹² One example on the fundamental principle of judicial review that may lead to a more limited analysis compared to the analysis carried out in light of the principle of proportionality is the reasonableness principle. Based on the latter principle, the question is the extent to which the Secretary of State was reasonable in issuing a data retention notice, which is seemingly different from considering whether a balancing act is struck in imposing a data retention obligation taking into account the data to be retained and its contribution to maintaining public safety. See Phoebe Hirst, 'Mass Surveillance in the Age of Terror: Bulk Powers in the Investigatory Powers Act 2016' (2019) 4 *European Human Rights Law Review* 403; Kosta, 'The Retention of Communications Data', 22.

¹⁹³ IPCO, *Advisory Notice 1/2018 Approval of Warrants, Authorisations and Notices by Judicial Commissioners* (8 March 2018), <https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/20180403-IPCO-Guidance-Note-2.pdf>.

¹⁹⁴ *Ibid.*, para. 19, p. 5.

¹⁹⁵ IPA, s. 77.

¹⁹⁶ IPA, s. 26 (for interception warrant) and s. 111 (for equipment interference).

¹⁹⁷ For example, according to s. 112(4)(a) of the IPA, where an equipment interference warrant authorises interference with equipment for obtaining legal privilege items, there must be exceptional and compelling circumstances to necessitate such authorisation. The same conditions must be satisfied where an interception warrant is issued to select items subject to legal privilege. For additional conditions relating to journalistic sources, see IPA, s. 29 (for interception warrants) and s. 114 (for equipment interference).

protect freedom of expression.¹⁹⁸ Following this decision, another Article 10 claim involving the same investigatory powers resulted in a friendly settlement because the UK government conceded that the legal regime preceding the IPA was not compliant with the Article 10 right and the Article 8 right.¹⁹⁹

The third debate on the safeguards provided under the IPA relates to the notification of individuals who may have been subjected to LEAs' and intelligence agencies' use of investigatory powers. According to section 231 of the IPA, the IPC must inform any person affected by errors in the use of investigatory powers laid out in the Act. As noted by Woods, this notification requirement is crucial for enabling individuals to make a complaint before the IPT, but there is a slight discrepancy with the notification requirement sought by the ECtHR.²⁰⁰ Accordingly, individuals must be notified of surveillance practices when those practices have ended if doing so does not prejudice the purpose of those practices.²⁰¹ Thus, the notification requirement as recognised by the ECtHR is not limited to cases involving 'serious errors' as required by the IPA. The wording of the notification requirement under the Act thus raised concerns about whether it undermines the potential for individuals to seek legal redress before the IPT, even though they can make a complaint before the Tribunal on a 'suspicion' of being subjected to investigatory powers under the IPA.²⁰² Despite these concerns, the ECtHR has not considered the absence of notification (in all cases, not limited to those involving 'serious error') a breach of the Article 8 right in and by itself so long as there is an effective *ex post* remedy.²⁰³

In addition to the specific safeguards included in the IPA, Part 3 of DPA 2018 can serve as a general framework for the rules and safeguards relating to the processing of personal data by UK LEAs in the context of criminal investigations. This Part of the 2018 Act transposes the EU's Law Enforcement Directive (LED)²⁰⁴ and sets out data protection principles with which the LEAs comply when processing personal data for law enforcement purposes. It also provides data subject rights about such processing.

Finally, restrictions to judicial redress may arise where the information obtained through mandatory or voluntary cooperation with service providers is used as evidence upon which a suspect is to be tried. The key legislation in this regard is the Criminal Procedure and Investigations Act 1996. This information will be disclosed to the suspect if it is not the subject of a relevant minister's application for a public interest immunity certificate relating to the case. Upon that application, a court may grant a certificate to withhold the information if (i) there is a countervailing public interest, (ii) non-disclosure is strictly necessary to protect this interest and (iii) any difficulty caused to the defence can be sufficiently counterbalanced to ensure a fair trial.²⁰⁵ Thus, to the extent that the information is not disclosed to suspects due to the existence of this certificate, he or she is not able to effectively verify whether the cooperation rules have been respected.

¹⁹⁸ *Big Brother Watch v. the UK*, Appl. Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, para. 456.

¹⁹⁹ *Human Rights Watch v. the UK*, Appl. No. 64230/16, 10 March 2022.

²⁰⁰ Lorna Woods, 'The Investigatory Powers Act 2016' (2017) 3 *European Data Protection Law Review* 103, 104.

²⁰¹ *Kennedy v. the UK*, para. 167; *Roman Zakharov v. Russia*, Appl. No. 47143/06, 4 December 2015, para. 289.

²⁰² Woods, 'The Investigatory Powers Act 2016', 104.

²⁰³ *Big Brother Watch v. the UK*, para. 359.

²⁰⁴ Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, [2018] OJ L119, 4 May 2016.

²⁰⁵ *R v. H and C* [2004] UKHL 3.

20.5 CROSS-BORDER COOPERATION BETWEEN LEAS AND SERVICE PROVIDERS

20.5.1 Introduction

This section provides an account of the legal basis for cross-border cooperation between LEAs and foreign service providers. Section 20.5.2 will consider the legal framework setting out the UK's mutual assistance obligations in the area of criminal investigations. Cross-border cooperation may take place as a result of the extraterritorial effect of laws prescribing investigatory powers to the LEAs. On this point, a distinction can be made between those powers prescribed by the IPA and the other investigatory powers found across different legislation. In relation to the former, as mentioned earlier, telecommunications operators based outside the UK may be compelled to comply with the duties set out in the IPA so long as they provide telecommunication services to a person located in the UK.²⁰⁶ Thus, based on this link to the UK, the investigatory powers under the IPA may have extraterritorial effects.²⁰⁷

Unlike the IPA, the other investigatory powers mentioned in Section 20.4.3.4 do not have such extraterritorial effects. The starting point in this regard is the jurisdictional limitations of the exercise of police powers found under the relevant statutes. In the UK, the police are primarily responsible for criminal law enforcement, and they derive their investigative powers from the Police Act 1997. The structure of the UK police can be subdivided into national and territorial bodies, the latter reflecting the different regions within England and Wales, Scotland and Northern Ireland. This is due to the peculiarity of the UK criminal jurisdiction, whereby the criminal legal system in England and Wales differs from the systems operating in Scotland and Northern Ireland.²⁰⁸ The jurisdictional power of the police can be found in the Police Act 1996, according to which '[a] member of a police force shall have all the powers and privileges of a constable throughout England and Wales and the adjacent United Kingdom waters'.²⁰⁹ There may also be other (express or implied) jurisdictional limitations for other law enforcement authorities.²¹⁰ Based on these jurisdictional limitations, information outside the territorial reach of UK LEAs should be obtained through mutual recognition instruments unless otherwise stated in statutes.

A prominent question is the impact of this jurisdictional limitation on LEAs' powers of search under PACE. According to this Act, a constable may require 'any information which is stored in any electronic form and is *accessible* from the premises to be produced in a form in which it can be taken away'.²¹¹ The wording of this provision may suggest an extraterritorial reach for the police's power of search to access and remove files from computer files based outside the UK if electronic data is accessible from the premises being searched.²¹² However, this search power must be read alongside the jurisdictional limitation under the Police Act 1996 described just now. This means that if the police access computer systems extraterritorially, they would be exercising their powers outside their jurisdiction.²¹³ For this reason, the police exercising their

²⁰⁶ Section 20.4.2 of this chapter.

²⁰⁷ Ibid.

²⁰⁸ However, for the purposes of this chapter, references to the UK refer primarily to England and Wales.

²⁰⁹ Police Act 1996, s. 30(1). A constable is the lowest-ranking police officer in the UK.

²¹⁰ For example, the Crime and Courts Act 2013, at Sch. 5, Pt 4, para. 12, provides explicit territorial restrictions for the National Crime Agency.

²¹¹ PACE, s. 20 [emphasis added].

²¹² Ian Walden, *Computer Crimes and Digital Investigations* (Oxford: Oxford University Press, 2016), 327.

²¹³ Ibid., 328.

powers to access computer systems under PACE must be mindful not to seize electronic data extraterritorially because UK courts may exclude it as unlawfully obtained evidence.²¹⁴

20.5.2 *Cooperation of National LEAs with Foreign Service Providers*

20.5.2.1 Legal Framework

This section considers the mandatory cooperation duties of foreign service providers with LEAs as laid out in UK law on mutual legal assistance (MLA) and in the UK's bilateral agreements with other countries. The section also provides a brief account of the Council of Europe Cybercrime Convention (Cybercrime Convention) to highlight how the investigatory powers discussed in Sections 20.3 and 20.4 enable the UK to comply with its obligations under the Convention.

20.5.2.1.1 **MUTUAL LEGAL ASSISTANCE.** The Crime (International Co-operation) Act 2003 (CICA) provides the general framework for mutual assistance in criminal matters, including obtaining evidence from abroad or assisting overseas authorities with obtaining evidence from the UK. There are many bilateral agreements to which the UK is a party.²¹⁵ These include bilateral MLA agreements (on restraint and confiscation or drug trafficking) with several EU member states (i.e., Italy, Spain and Sweden). It also has an MLA agreement with Ireland. These treaties do not specifically relate to interception of electronic communication but rather include provisions on the exchange of information and/or intelligence about criminal investigations relating to specific offences (e.g., drug trafficking) or about the exercise of specific investigatory powers (e.g., restraint and confiscation of proceeds of crimes).

Following the enactment of the CLOUD Act in the US, the UK legal landscape has changed to enable outgoing requests from UK LEAs to US-based service providers. First, the Crime (Overseas Production Order) Act 2019 (COPOA) was enacted to provide the national legal basis for the implementation of the UK–US Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime (UK–US Agreement).²¹⁶ Signed in October 2019 and operational since 3 October 2022, the UK–US Agreement is seen as the first example of a shift away from traditional MLA treaties.²¹⁷ Section 20.5.2.3 gives a brief account of COPOA.

Finally, the UK's withdrawal from the EU has changed the channel of cooperation between the UK and the EU member states on MLA since the UK can no longer participate in EIOs after the end of the transition period on 31 December 2020. The EIOs received before this date will still be processed, but any EIO received afterwards will be processed as an MLA request. Requests as such are now based on the EU–UK Trade and Cooperation Agreement (TCA), which is based on the Council of Europe 1959 Convention on Mutual Assistance in Criminal Matters and its protocols.²¹⁸

²¹⁴ PACE, s. 78.

²¹⁵ See Home Office, 'List of UK Bilateral Treaties on Mutual Legal Assistance in Criminal Matters', 7 March 2022, www.gov.uk/government/publications/bilateral-treaties-on-mutual-legal-assistance-in-criminal-matters.

²¹⁶ Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington, 3 October 2019, USA No. 6 (2019), CP 178 (UK–US Agreement).

²¹⁷ Jean Galbraith, 'United States and United Kingdom Sign the First Bilateral Agreement Pursuant to the CLOUD Act, Facilitating Cross-Border Access to Data' (2020) 114(1) *American Journal of International Law* 124.

²¹⁸ Title VIII, Part 3 of the EU–UK Trade and Cooperation Agreement (TCA) governs the rules and procedures for EU–UK MLA. For commentary, see Anna Oechmichen and Ben Keith, 'Mutual Legal Assistance under the EU–UK Trade and Cooperation Agreement' (2021) 12(2) *New Journal of European Criminal Law* 222.

20.5.2.1.2 THE COUNCIL OF EUROPE CYBERCRIME CONVENTION. The UK signed the Cybercrime Convention in November 2001 and ratified it in May 2011. The Convention entered into force in September 2011. This late ratification was because the then-existing UK law, specifically the CMA 1990, required amendments to align its provisions with the Convention. Such statutory amendment did not occur until 2006, through the Police and Justice Act 2006, while the relevant provisions did not enter into force until 1 October 2008.

Despite its late ratification, the Cybercrime Convention was not widely controversial.²¹⁹ That said, the UK made certain reservations to the articles of the Cybercrime Convention on the criminalisation of images appearing to show a minor engaged in sexual conduct, as well as jurisdiction and MLA.²²⁰ The Cybercrime Convention provisions are dispersed through different statutes. Rules requiring the preservation of data (Articles 16 and 17) are found in PACE. In addition, a preservation request from a foreign law enforcement agency can be made under the CICA, already discussed in Section 20.5.2.1.1. Rules requiring the production of data (Article 18(1)(a)) are found in various pieces of UK legislation, including PACE, the Terrorism Act 2000, the Proceeds of Crime Act 2002 and the IPA, which have been explored in Sections 20.3 and 20.4. General powers of search and seizure (Article 19) are contained in PACE, discussed in Section 20.4.3.4. The real-time collection of data (Articles 20 and 21) from a service provider through interception is governed by the IPA under its process of interception of the content of communications, discussed in Section 20.4.3.1. In some areas, the UK law goes beyond the Convention's provisions on procedural law. For example, as explored in Section 20.2.2, the IPA addresses both public and private telecommunications providers. It also provides for a data retention scheme, which is discussed in Section 20.3.2.

20.5.2.2 Nature of Cooperation

According to the report of the Independent Reviewer of Terrorism Legislation on the investigatory powers of LEAs before the IPA, cooperation between UK law enforcement and overseas service providers had been entirely voluntary.²²¹ However, following the Snowden revelations in 2013 on global surveillance programmes, the degree of cooperation diminished and differed between service providers.²²² In addition, US service providers did not voluntarily cooperate in respect of interception due to the obligations under US Federal laws.²²³ The report also noted that the sharing of subscriber data had been more common.²²⁴

Apart from this report, there is no information published by UK public authorities documenting statistics on the extent to which LEAs cooperate with foreign service providers. However, the transparency reports of the largest service providers do provide some indication of how frequently UK LEAs make requests for data.²²⁵ For example, according to Google's "Transparency

²¹⁹ All Party Internet Group (APIG), 'Revision of the Computer Misuse Act': Report of an Inquiry by the All Party Internet Group (June 2004), para. 82, www.cl.cam.ac.uk/~mci/APIG-report-cma.pdf.

²²⁰ Council of Europe, Reservations and Declarations for Treaty No. 185 – Convention on Cybercrime (ETS No. 185), www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=o.

²²¹ Anderson, *A Question of Trust*, para. 11.18, p. 207.

²²² *Ibid.*, para. 11.5, p. 203.

²²³ *Ibid.*, para. 11.18, p. 207.

²²⁴ *Ibid.*

²²⁵ See Yahoo, 'Transparency Report', <https://transparency.yahoo.com>; Twitter, 'Transparency', <https://transparency.twitter.com>.

Report', the UK made 7,896 requests for subscriber data and 6,699 other legal requests from July 2020 to December 2020.²²⁶

20.5.2.3 Overview of Existing Cooperation Duties

The CICA governs the rules and procedures for obtaining evidence through the relevant authorities of the jurisdiction in which the evidence resides. Non-UK-based service providers thus may be requested to provide information based on a request made according to this Act. A judge, on the application of a prosecuting authority (e.g., the Crown Prosecution Service) or a person charged in the proceedings (i.e., the defendant), may issue a request for evidence from abroad.²²⁷ This request may be made only if an offence has been committed or there are reasonable grounds for suspecting that an offence has been committed, and proceedings for that offence have been instituted or an investigation is underway.²²⁸ The request may be sent to a court in the relevant jurisdiction, to an authority designated in the jurisdiction for receipt of such requests or, in cases of urgency, to the International Criminal Police Organization (INTERPOL).²²⁹ The evidence, once received, should then be used only for the purpose specified in the request, a rule which is known as the 'speciality principle'.²³⁰ Requests for UK-based evidence by overseas authorities must be sent to the Secretary of State at the Home Office, referred to as the 'territorial authority'.²³¹ The Secretary of State may then nominate a court to receive the requested evidence. As well as achieving the disclosure of particular evidence, the MLA procedure also provides for the obtaining of evidence. The Secretary of State may direct that a warrant be applied for from the courts so that a search can be undertaken and evidence seized. However, such coercive powers may be exercised only where the conduct constitutes an appropriate offence both in the requesting country and under the laws of England and Wales (the so-called double criminality principle), as also required in extradition proceedings.

The COPOA provides another regime to allow obtaining electronic data residing in a foreign jurisdiction.²³² It introduces a procedure in which law enforcement authorities may apply for an 'overseas production order' from a Crown Court judge requiring persons operating outside the UK to produce or grant access to specified electronic data. Items subject to legal privilege or a confidential personal record are 'excepted electronic data';²³³ as is 'communications data' held by a telecommunications operator, as defined under the IPA, which cannot be sought by a COPOA order.²³⁴

Upon an application by the 'appropriate officer' (which includes a constable, an accredited financial investigator or any person specified in regulations)²³⁵ under a 'designated international cooperation arrangement', a judge may issue an order if he or she is satisfied that the data was likely to be of substantial value to the criminal proceedings or investigation for which it was

²²⁶ Google, 'Transparency Report for the UK', https://transparencyreport.google.com/user-data/overview?hl=en_GB&user_requests_report_period=series:requests,accounts;authority:GB;time:&lu=legal_process_breakdown&legal_process_breakdown=expanded:o.

²²⁷ CICA, ss. 7–12.

²²⁸ Ibid., s. 7(1).

²²⁹ Ibid., s. 8.

²³⁰ Ibid., s. 3(7).

²³¹ Ibid., ss. 13–28(9).

²³² COPOA, s. 3(1), defines 'electronic data' as 'data stored electronically'.

²³³ COPOA, s. 3(2).

²³⁴ Ibid., s. 3(4).

²³⁵ Ibid., s. 2(1).

being requested and that it would be in the public interest.²³⁶ To date, the only ‘designated international cooperation arrangement’ is the UK–US Agreement.²³⁷ An order under the Act can be issued only for an indictable offence, that is, an offence that must be tried before the Crown Court and thus cannot be tried before a magistrates’ court.

In essence, the UK–US Agreement incorporates the conditions and standards provided in the second part of the CLOUD Act on requesting data directly from US-based providers.²³⁸ There is a difference in terms of when the UK authorities and the US authorities may seek an order under the Agreement based on the nationality and the place of residence of the target. Orders issued by the US authorities cannot target people residing in the UK or legal persons registered in the UK.²³⁹ On the face of this limitation, these orders can target UK citizens so long as they reside outside the UK. On the other hand, orders issued by the UK authorities cannot target US citizens, US residents or legal persons registered in the US.²⁴⁰ This type of differential treatment on the subject scope of orders has called the ‘reciprocity’ of the UK–US Agreement into question.²⁴¹

Another piece of legislation governing cooperation with non-UK-based service providers is the IPA, which contains provisions allowing the relevant UK authority to serve an interception warrant,²⁴² a data retention notice,²⁴³ a data acquisition authorisation,²⁴⁴ an equipment interference warrant²⁴⁵ or a technical capability notice²⁴⁶ to a telecommunications operator outside the UK based on the provision of telecommunications services to persons in the UK or telecommunication systems in the UK.²⁴⁷ However, the IPA recognised the enforcement limitations against foreign service providers, so the Secretary of State does not have the power to start civil proceedings to enforce the duty to comply with the requirement and responsibilities laid out in equipment interference warrants,²⁴⁸ data retention notices²⁴⁹ or technical capability notices²⁵⁰ against a telecommunications operator based outside the UK.

²³⁶ Ibid., s. 4(2)–(7).

²³⁷ Overseas Production Orders and Requests for Interception (Designation of Agreement) Regulations 2020/38 (Regulations 2020/38).

²³⁸ Theodore Christakis, ‘21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How It Works – with Charts)’, European Law Blog, 17 October 2019, <https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/>.

²³⁹ UK–US Agreement, Art. 1.

²⁴⁰ Ibid.

²⁴¹ Christakis states that the difference on the personal scope of the orders was due to the impact of EU law, by which the UK was still bound by at the time, prohibiting discrimination against EU citizens, but the author challenges the reciprocity and limitation provisions of the UK–US Agreement where the first part of the CLOUD Act remains in effect, and warns that it may be used to bypass the provisions of the UK–US Agreement. Similarly, according to the author, the extraterritorial provisions of the IPA and the COPOA may be utilised by the UK authorities to bypass the UK–US Agreement, as well. See Christakis, ‘21 Thoughts and Questions’.

²⁴² IPA, s. 42(3).

²⁴³ IPA, s. 97(1). Only when the Investigatory Powers (Amendment) Act 2024, s. 17, is implemented.

²⁴⁴ IPA, s. 85(2).

²⁴⁵ IPA, s. 126(3).

²⁴⁶ IPA, s. 253(8).

²⁴⁷ See Section 20.2.2 of this chapter. There is a presumption under UK law against the extraterritorial exercise of UK investigatory powers where an entity is not carrying on business in the UK. See *R (KBR, Inc) v. Director of the Serious Fraud Office* [2021] UKSC 2. See also Tim Cochrane, ‘The Presumption against Extraterritoriality, Mutual Legal Assistance, and the Future of Law Enforcement Cross-Border Evidence Collection’ (2022) 85(2) *Modern Law Review* 526.

²⁴⁸ IPA, s. 128(7).

²⁴⁹ IPA, s. 97(2).

²⁵⁰ IPA, s. 255(10).

On the contrary, an interception warrant²⁵¹ and a notice for the acquisition of communications data²⁵² may be enforced by civil proceedings irrespective of the location of the telecommunications operator. That said, to date, there are no examples of such enforcement action. This is likely due to concerns about publicity and disrupting the culture of negotiating arrangements, which was highlighted in Section 20.4.2. In addition, express acknowledgement of the potential for conflict of laws serves as a defence against compliance by a telecommunications operator in these circumstances.²⁵³

20.5.2.4 Legal Remedies and Protection of Human Rights

This section focuses on the legal remedies and protection of human rights available under the US–UK Agreement and Title VIII of Part 3 of the EU–UK TCA on MLA, other than the remedies and safeguards available under UK law, which have been discussed in Section 20.4.4. As much as the UK–US Agreement itself was praised for being a ‘blueprint’ for future executive agreements,²⁵⁴ the standard of privacy and the data protection safeguards, as well as the legal remedies available to the subjects of orders issued by US authorities have been criticised.²⁵⁵ The Agreement contains a separate provision for privacy and data protection safeguards, which refers to the EU–US Umbrella Agreement and the applicable privacy and data protection laws of the UK and the US.²⁵⁶ However, it does not contain specific notification requirements for the subjects of orders; nor does it provide an independent oversight body to resolve the disputes except for allowing service providers to object to an order.²⁵⁷ There is no mechanism for addressing conflicts of laws.²⁵⁸ The positive side of the Agreement could be that production orders ‘shall be subject to review or oversight under the domestic law of the Issuing Party by a court, judge, magistrate, or other independent authority’.²⁵⁹ The designated authority of the issuing party, who will transmit the order to the service provider, should review and certify the compliance of the order with the Agreement.²⁶⁰

As regards the standard of human rights protection and the legal remedies available under Title VIII of the EU–UK TCA, while this title is largely based on the 1959 Convention, certain features of the EIO are also included in it. The most praised feature in this regard is that the requested state should factor in the necessity and the proportionality of the request for the proceedings.²⁶¹ However, the specific provisions relating to MLA do not refer to a right to legal remedy. Nevertheless, the references to the commitment to protect human rights and fundamental freedoms on which the law enforcement cooperation is based may serve as the UK’s commitment to the right to a legal remedy as enshrined in Article 6 of the ECHR.²⁶²

²⁵¹ IPA, s. 43(8).

²⁵² IPA, s. 66(5).

²⁵³ IPA, ss. 43(5) and 85(4).

²⁵⁴ Jennifer Daskal and Peter Swire, ‘The UK-US Cloud Act Agreement Is Finally Here, Containing New Safeguards’, *Law Fare*, 8 October 2019, www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards.

²⁵⁵ Sergio Carrera, Marco Stefan and Valsamis Mitsilegas, ‘Cross-Border Data Access in Criminal Proceedings and the Future of Digital Justice: Navigating the Current Legal Framework and Exploring Ways Forward within the EU and across the Atlantic’, Centre for European Policy Studies (CEPS), 14 October 2020, www.ceps.eu/ceps-publications/cross-border-data-access-in-criminal-proceedings-and-the-future-of-digital-justice/.

²⁵⁶ UK–US Agreement, Art. 9(2).

²⁵⁷ *Ibid.*, Art. 5.

²⁵⁸ Christakis, ‘21 Thoughts and Questions’.

²⁵⁹ UK–US Agreement, Art. 5(2).

²⁶⁰ *Ibid.*, Art. 5(6)–(7).

²⁶¹ EU–UK TCA, Art. 636.

²⁶² Oechmichen and Keith, ‘Mutual Legal Assistance under the EU–UK Trade and Cooperation Agreement’, 222, 229.

20.5.3 *Cooperation of National Service Providers with Foreign LEAs*

National service providers may cooperate with foreign LEAs in the interception of communications based on a mutual assistance warrant issued by the Secretary of State.²⁶³ In the absence of such a warrant, a request for the interception of communications by a foreign authority would be lawful only if carried out by a telecommunications operator; the request is made in accordance with the terms of a ‘relevant international agreement’, and the target is, or is believed to be, outside the UK.²⁶⁴ To date, the only such international agreement is the UK–US Agreement, which entered into operation on 3 October 2022.

With regard to the transfer of stored communications data to foreign authorities by national service providers, there is no explicit prohibition against that transfer under the IPA. Nevertheless, service providers may be prevented from any such cooperation based on UK data protection legislation. According to the UK General Data Protection Regulation (GDPR), personal data must not be transferred outside the UK unless certain conditions exist.²⁶⁵ As mentioned earlier, the UK GDPR follows the rules and principles under the EU’s GDPR, and these conditions are equivalent to the data transfer rules under the latter. As regards transfers to EU member states, the DPA contains transitional provisions that recognise that transfers to a European Economic Area (EEA) state or to a third country subject to a European Commission adequacy decision are permissible.²⁶⁶

20.6 CONCLUSION

This chapter has offered an examination of the UK legal framework governing the duties of service providers to cooperate with LEAs in obtaining digital evidence. Much of the analysis focused on the investigatory powers under the IPA, including amendments made to reflect judicial decisions. An important aspect of these powers in relation to obtaining digital evidence is that the IPA prescribes territorial jurisdiction broadly, resulting in an extraterritorial effect for foreign telecommunications operators that provide telecommunication services to persons, or control telecommunication systems, in the UK. Despite this extraterritorial effect, the ability of the UK government to enforce such obligations against telecommunications operators outside the UK is inevitably constrained.

Other UK investigatory powers contain jurisdictional limitations by which LEAs that exercise their powers outside the jurisdiction would be *ultra vires*. The greatest change in UK law concerning obtaining digital evidence from abroad has been developments around the UK–US Agreement and the COPOA. These now allow UK LEAs to request digital evidence directly from a US service provider in certain circumstances.

²⁶³ IPA, s. 15(4).

²⁶⁴ IPA, s. 52.

²⁶⁵ UK GDPR, Ch. 5, and DPA 2018, ss. 73–76.

²⁶⁶ DPA, Sch. 21, Pt 3, paras. 4–6.

Digital Evidence Gathering by US Authorities and Cross-Border Cooperation with US-Based Service Providers

*Marine Corhay and Vanessa Franssen**

21.1 INTRODUCTION

Law enforcement entities – not just from the United States but from around the world – seek data in the hands of US-based internet service providers. In the first six months of 2021 alone, Google received more than 149,000 requests for user information, covering more than 359,000 accounts.¹ During that same time period, Facebook received some 211,000 requests, also with well over two-thirds coming from non-US authorities.² Twitter (now X) received approximately 12,000 requests, three-quarters of which were issued by authorities outside the United States.³ This chapter provides an account of the governing legal framework with respect to the gathering of digital evidence by US authorities and the rules that bind US service providers – an issue that, given the quantity of data of interest in the hands of US-based providers, increasingly matters to law enforcement entities all around the world.

At the national level, US law enforcement is bound by the Fourth Amendment to the US Constitution. The Fourth Amendment's dictates, which are shaped by the relevant court interpretations, are supplemented by the Electronic Communications Privacy Act (ECPA), the key governing statute covering law enforcement access to data.⁴ The ECPA sets limits on what information US-based service providers can voluntarily share with both US and foreign authorities. It also sets out the substantive and procedural rules by which US law enforcement can compel production from such providers. Separate state laws can, and in some cases do, provide additional limits and protections with respect to electronic data. State law, however, cannot *lessen* the protections governing the collection and use of data provided for by federal statutory and constitutional law.⁵ This chapter

* This chapter is based on a draft country report written by Jennifer Daskal, Professor and Faculty Director, Tech, Law & Security Program, American University Washington College of Law, based on the state of law end 2019. After Prof. Daskal joined the Biden administration in January 2021, she was unable to finalize and publish the text under her name without institutional approval. Therefore, it was agreed that Vanessa Franssen, as co-editor of this volume, and PhD researcher Marine Corhay would update the text and publish it under their names. While any mistake or error is our sole responsibility, we are deeply indebted to Jennifer for her excellent work. Special thanks to Daniel de Zayas for the excellent research assistance, and to Peter Swire for his valuable comments.

¹ Global requests for user information, Google Transparency Report, <https://transparencyreport.google.com/user-data/overview?hl=en>.

² Government Requests for User Data, Meta Transparency Report, <https://transparency.fb.com/data/government-data-requests/>.

³ Information Requests, Twitter Transparency Report, <https://transparency.twitter.com/en/information-requests.html>.

⁴ Separate statutory provisions govern collection for foreign intelligence purposes. Those are outside the scope of this discussion.

⁵ On October 8, 2015, California adopted its own separate statute governing access to stored communications – the California Electronic Communications Privacy Act (CalECPA) – that imposes more stringent requirements and protections than the federal statute. California Penal Code § 1546 *et seq.* (1872). See also California Assembly

focuses on the national rules that bind all US-based providers, regardless of their location within the United States, as well as all federal, state and local law enforcement authorities.

This chapter delves into these rules in more detail. Sections 21.2 and 21.3 describe the general statutory and constitutional scheme governing data collection in the United States, with a focus on the federal level. Section 21.4 examines specific questions with respect to cross-border cooperation, particularly in light of widely discussed legislation enacted in March 2018 – the Clarifying Lawful Overseas Uses of Data (CLOUD) Act⁶ – that seeks to better facilitate cross-border access to data, in specified circumstances and in accordance with baseline procedural and substantive protections. Finally, Section 21.5 draws some concluding thoughts about both the need for more attention to cross-border access to data and some of the lacuna in US law. As discussed in this final section, most of the applicable constitutional and statutory provisions focus on governmental acquisition, with relatively little in the way of statutory or constitutional limits on retention or use once data has been acquired by governmental entities.

21.2 THE CONSTITUTIONAL FRAMEWORK

The key constitutional rule governing law enforcement access to data is the Fourth Amendment: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” Notably, the Fourth Amendment does not give governmental agents affirmative authority or the right to any particular piece of information or data. Rather, it sets *limits* on governmental actions that seek to access such information – specifying that searches and seizures must be “reasonable” and that warrants be issued pursuant to the specified requirements, including probable cause and specificity as to the area being searched or the thing to be seized. The probable cause requirement is effectively a standard of proof requirement – requiring the law enforcement agent to proffer to the satisfaction of a reviewing judge facts and circumstances within a government agent’s knowledge and based upon trustworthy information to support a reasonable finding that an offense has been or is being committed.⁷

What constitutes a “search” or “seizure” for the purposes of the Fourth Amendment has been – and continues to be – subject to ongoing litigation, debate and development. For years, the Supreme Court required some sort of physical trespass into a constitutionally protected area (i.e., the home) as a prerequisite for triggering the Fourth Amendment’s protections.⁸ This led to some strange anomalies. Agents could listen in on phone and even in-person conversations as long as they did so using technology that did not trespass into the home or other protected space;

Committee on Privacy & Consumer Protection, Bill Analysis, SB 178, 2015–2016 Leg., Reg. Sess., at 4, <https://perma.cc/UXS2-X9KP>. For more information about CalECPA’s passage, see Susan Freiwald, “At the Privacy Vanguard: California’s Electronic Communications Privacy Act (CalECPA)” (2018) 33 *Berkeley Technology Law Journal* 131, 150–153. It specifies that state law enforcement must generally obtain a warrant for a broader range of data than explicitly required by federal law. Only a relatively narrow category of “subscriber information” – defined as “name, street address, telephone number, email address, or similar contact information . . . account number or identifier, the length of service, and the types of services used” – is exempted from the warrant requirement. Cal. Penal Code § 1546.1.

⁶ Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018, www.justice.gov/dag/page/file/1152896/download.

⁷ *Brinegar v. United States*, 338 US 160, 175–176 (1949).

⁸ *Olmstead v. United States*, 277 US 438, 457, 466 (1928) (affirming that the Fourth Amendment cannot be violated “unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house ‘or curtilage’ for the purpose of making a seizure”).

if, however, the listening device physically touched the home, then the surveillance was unlawful.⁹

The landmark 1967 case *Katz v. United States* changed this, establishing that the Fourth Amendment protects “people, not places” and adopting a “reasonable expectation of privacy” test that supplemented (although did not supplant) the trespass test. As a result, law enforcement officers could no longer listen in on phone conversations without a warrant.¹⁰ The now applicable reasonable expectation of privacy test requires that: (i) individuals demonstrate a subjective expectation of privacy; and (ii) it is something that is considered to be reasonable.¹¹ But this test, too, is subject to a large number of very valid critiques. As several scholars have noted, the test itself is circular, and what is considered to be protected (or not) is ever evolving. It depends on societal expectations, which in turn depend, in part, on technological developments and, in part, on what the courts conclude are reasonable societal expectations while adjudicating particular cases.¹²

The third-party doctrine, a corollary to the reasonable expectation of privacy test, stands for the proposition that when someone voluntarily shares information (including personal data) with a third party, he or she no longer has a subjective expectation of privacy. As the Supreme Court put it in the 1976 case of *United States v. Miller*, individuals lack a reasonable expectation of privacy in information “revealed to a third party and conveyed by [that third party] to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.”¹³ Based on this doctrine, courts have concluded that anything from bank records to phone numbers dialed and received, to videos from surveillance tapes, to privately held location data was not protected by the Fourth Amendment, and thus could be acquired by the government without being subject to the strictures of the Fourth Amendment.¹⁴

⁹ Compare, *Goldman v. United States*, 316 US 129, 131–132, 134–135 (1942) (holding that the placement of a detectaphone against a wall to amplify conversations on the other side did not constitute an illegal trespass and, therefore, did not constitute an unlawful search), and *Olmstead* at 457, 466 (holding that the government does not conduct a search when it wiretaps telephone lines leading to, but not located on, the defendant’s property), with *Silverman v. United States*, 365 US 505, 509, 512 (1961) (holding that a spike mike penetrating the defendant’s heating duct constituted an “actual intrusion into a constitutionally protected area” and, therefore, violated the Fourth Amendment).

¹⁰ *Katz v. United States*, 389 US 347, 351, 356–359 (1967) and 360–361 (Harlan, J., concurring).

¹¹ *Katz*, 361 (Harlan, J., concurring).

¹² *United States v. Jones*, 565 US 400, 427 (2012) (Alito, J., concurring) (“[T]echnology can change [privacy] expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes.”); *Kyllo v. United States*, 533 US 27, 34–35 (2001) (acknowledging technology’s influence upon expectations of privacy and questioning “what limits there are upon this power of technology to shrink the realm of guaranteed privacy”). For further discussion of criticisms of the reasonable expectation of privacy test, see Orin S. Kerr, “Katz Has Only One Step: The Irrelevance of Subjective Expectations” (2015) 82 *University of Chicago Law Review* 113, 114 (arguing that the Supreme Court has deteriorated the role of the subjective expectation of privacy, leaving only an inquiry as to whether the expectation of privacy is reasonable); Jed Rubenfeld, “The End of Privacy” (2008) 61 *Stanford Law Review* 101; Silas J. Wasserstrom and Louis Michael Seldman, “The Fourth Amendment as Constitutional Theory” (1988) 77 *Georgetown Law Journal* 19, 69 (attributing the test’s “notorious circularity” to the belief that the Constitution embodies reasonable expectations of how society actually functions); Richard A. Posner, “The Uncertain Protection of Privacy by the Supreme Court” (1979) *Supreme Court Review* 173, 188 (“[I]t is circular to say that there is no invasion of privacy unless the individual whose privacy is invaded had a reasonable expectation of privacy; whether he will or will not have such an expectation will depend on what the legal rule is.”).

¹³ *United States v. Miller*, 425 US 435, 443 (1976); see also *Smith v. Maryland*, 442 US 735, 743–745 (1979).

¹⁴ See, e.g., *Smith* at 745 (finding no expectation of privacy in phone numbers dialed, and thus no search under the Fourth Amendment, because the numbers are “voluntarily conveyed” to the telephone company and the phone user “assume[s] the risk” that the company would convey them to the police); *Miller* at 443 (finding no expectation of privacy in financial statements and deposit slips “voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business”); *United States v. Davis*, 785 F.3d 498, 517–518 (11th Cir. 2015) (finding no expectation of privacy in historical cell-site location information “made, kept, and owned” by telephone companies); *United*

That said, the US Supreme Court's June 2018 decision in *Carpenter v. United States*, while purporting to leave the third-party doctrine intact, began to set some doctrinal limits. Specifically, the Court held that collection of seven days or more of historical cell-site location data – data that reveals a person's whereabouts – is a “search” that triggers the Fourth Amendment, even though that data had been shared with and collected by the third-party cell phone provider.¹⁵ The case similarly establishes that the content of emails is generally covered by the Fourth Amendment. Logically speaking, a range of other communications content, including text messaging, instant messaging and other forms of non-public, person-to-person communication via social media, should also be understood as subject to the Fourth Amendment's protections.¹⁶ In the wake of the *Carpenter* ruling, the question of what categories of data in the hands of third-party service providers are protected by the Fourth Amendment remains a hotly contested question – one that will surely entail litigation¹⁷ and debate for years to come.¹⁸

Some first answers can be found in the following judgments. In *United States v. Hood*, the First Circuit Court of Appeals declined to extend *Carpenter* in finding no expectation of privacy in internet protocol (IP) addresses associated with a mobile messaging app account. The Court distinguished IP addresses from cell-site location information on the grounds that IP addresses are voluntarily disclosed by a user's affirmative decision to access the internet and do not reveal location information.¹⁹ In *United States v. Shipton*, the District Court of Minnesota found no expectation of privacy in files on an individual's computer that are shared over a peer-to-peer file-sharing network, distinguishing *Carpenter* on the grounds that users voluntarily add the files to

States v. Longoria, 177 F 3d 1179, 1184 (10th Cir. 1999) (rejecting the existence of a reasonable expectation of privacy in audio and video conversations taped by an informant).

¹⁵ *Carpenter v. United States*, 138 S Ct 2206, 2217 and n. 3 (2018).

¹⁶ *Carpenter*, 2222 (expressing concerns that “private letters” that have been digitalized could be collected by anything other than a warrant) and 2269 (Gorsuch, J., dissenting) (“few doubt that e-mail should be treated much like the traditional mail it has largely supplanted”); see Paul Ohm, “The Many Revolutions of Carpenter” (2019) 32 *Harvard Journal of Law & Technology* 357, 358–361 (making this point).

¹⁷ See, e.g., *Naperville Smart Meter Awareness v. City of Naperville*, 900 F 3d 521, 527–529 (7th Cir. 2018) (holding that under *Carpenter* a government utility provider's constant collection of home energy-consumption data constituted a search, although finding such search to be reasonable under the circumstances); *United States v. Kelly*, 385 F. Supp. 3d 721, 726–730 (ED Wis. 2019) (holding that video surveillance of the exterior of an apartment did not constitute a search, distinguishing stationary video surveillance from surveillance “follow[ing] a person into homes, places of worship, hotels, bedrooms, restaurants, and meetings”); *State v. Sylvestre*, 254 So. 3d 986, 991–992 (Fla. Dist. Ct App. 2018) (holding that *Carpenter* requires the government to obtain a warrant to obtain real-time cell location information). For an empirical study of the post-*Carpenter* case law between 2018 and 2021, see Matthew Tokson, “The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018–2021” (2022) 135 *Harvard Law Review* 1790.

¹⁸ Susan Freiwald and Stephen Wm Smith, “The Carpenter Chronicle: A Near-Perfect Surveillance” (2018) 132 *Harvard Law Review* 205, 230 (forecasting that post-*Carpenter* courts will be required to determine whether individuals have a reasonable expectation of privacy in records related to purchase and browsing history, health, and fitness held in commercial databases); Orin S. Kerr, “Implementing Carpenter,” USC Law Legal Studies Paper No. 18-29 (2018), <https://ssrn.com/abstract=3301257> (arguing that *Carpenter* should require the government to obtain a warrant in order to obtain transactional records about how a messaging service was used and to monitor browsing history, but that no warrant should be required to obtain ride-sharing records or to monitor IP addresses); Alan Z. Rozenshtein, “Fourth Amendment Reasonableness After Carpenter” (2019) 128 *Yale Law Journal Forum* 943, 944 (positing that the Supreme Court in *Carpenter* missed the opportunity “to decide when legislatively authorized warrantless electronic surveillance is reasonable”); Daniel de Zayas, “Carpenter v. United States and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History” (2019) 68 *American University Law Review* 2209 (arguing that courts should interpret *Carpenter* as recognizing a reasonable expectation of privacy in browsing history); Margot E. Kaminski, “Carpenter v. United States: Big Data Is Different” (2018) *George Washington Law Review*, www.gwlr.org/carpenter-v-united-states-big-data-is-different.

¹⁹ *United States v. Hood*, 920 F 3d 87, 92 (1st Cir. 2019).

the network where the government is entitled to use hashing to identify illicit files.²⁰ Yet, many other elements of the *Carpenter* ruling remain a “mystery.”²¹

Even if broadly applied, there will continue to be a range of governmental actions that result in the review or acquisition of data and are neither searches nor seizures, as those terms have been defined, and thus fall outside the scope of the Fourth Amendment’s protections²² (although they may be covered by separate statutory rules and specified as in Section 21.3 of this chapter).²³ Indeed, the Fourth Amendment sets only a “floor for privacy protection,” which can be supplemented with additional legislative protections.²⁴

It should also be emphasized that Fourth Amendment doctrine sets territorial limitations on its scope. It provides protections to US citizens, legal permanent residents and others physically located within the United States. But it does not protect or otherwise limit US governmental activities with respect to non-citizens located outside the United States, absent a determination that the particular non-citizen has “substantial” voluntary connections to the United States.²⁵

Moreover, even in the context in which the Fourth Amendment does apply outside the territorial borders of the United States (e.g., if the United States government is engaging in a search or seizure of a US person who is located outside the United States), the specific protections provided will vary based on the context and the court’s determination as to what is “reasonable,” given the particular context. Among other key differences, the US government’s search of a residence overseas does not require issuance of a warrant.²⁶

21.3 THE STATUTORY FRAMEWORK

The key federal statutory rule governing law enforcement access to data is ECPA, which itself encompasses three distinct sections – the Stored Communications Act (SCA), the Wiretap Act and the Pen Register statute. The Communications Assistance for Law Enforcement Act (CALEA) separately sets out rules requiring telecommunication companies’ assistance in the execution of wiretaps. These statutes govern both federal and state law enforcement access to data, although, as described in Section 21.3.4, state law can adopt heightened protections that apply to state law enforcement beyond what is provided for by federal law. State law cannot lessen protections provided for under federal law.

21.3.1 *The Stored Communications Act*

The SCA (18 USC § 2701 *et seq.*) criminalizes unlawful access to stored wire and electronic communications and regulates the disclosure of such data. The law distinguishes along two key

²⁰ *United States v. Shipton*, No. 0:18-cr-202-PJS-KMM, 2019 WL 5330928, at *12–17 (D Minn. September 11, 2019). The District Court’s ruling was affirmed by the 8th Circuit Court of Appeals, No. 20-2570 on June 16, 2021.

²¹ Tokson, “The Aftermath of *Carpenter*,” 1804–1806 (stressing the important role of lower courts in applying and further elaborating *Carpenter*, contributing this way to a “precedential dialogue” with the Supreme Court).

²² According to a recent empirical study, “[c]ourts find Fourth Amendment searches in relatively few rulings, and federal courts find searches at substantially lower rates than state courts,” which is quite telling. See Tokson, “The Aftermath of *Carpenter*,” 1851.

²³ Kerr argues that content preservation orders under 18 USC § 2703(f) amount to a seizure and therefore should be subject to the same basic Fourth Amendment restrictions. See Orin S. Kerr, “The Fourth Amendment Limits of Internet Content Preservation” (2021) 65 *Saint-Louis University Law Journal* 743.

²⁴ Tokson, “The Aftermath of *Carpenter*,” 1851.

²⁵ *Verdugo v. United States*, 494 US 259, 271 (1990).

²⁶ *United States v. Odeh (In re Terrorist Bombings of United States Embassies in E. Afr.)*, 552 F 3d 157 (2d Cir. 2008); *United States v. Bin Laden*, 126 F Supp. 2d 264, 277 (SDNY 2000).

axes: the nature of the carrier and the nature of the data, with different rules applicable to communications content and non-content data. Non-content data is further divided into what is often referred to as subscriber information (including name, address, records of session times and durations, length of service, IP address and payment information, including credit card or bank account number) and other customer records – with different procedural and substantive rules governing law enforcement access.²⁷ As will be explained later in this section, non-content data under the SCA includes two categories of (stored) data, which somewhat resemble the distinction made by the Cybercrime Convention²⁸ between “subscriber information”²⁹ and “traffic data,”³⁰ yet without fully corresponding to the division lines drawn by this Convention.

The SCA’s rules apply to providers of an “electronic communication service” (ECS) and a “remote computing service” (RCS) (referred to herein as “covered providers”), with slightly different rules for each.³¹ An ECS is defined as any service which allows users the ability to send or receive wire or electronic communications.³² Examples of electronic communication services include email services, text messaging providers and social media networks.³³

An RCS is any service that maintains an electronic communications service for the purpose of data storage or processing.³⁴ Examples include cloud-based services that allow users to store documents or photos for retrieval or later use, including a service that permits users to upload, store and later review documents, photos and videos.³⁵ An RCS that permits users to send and receive communications content is also an ECS.³⁶ Moreover, as several US courts have concluded, even an entity that provides only ECS or RCS as part of its business is still covered by and subject to the disclosure limitations of the SCA.³⁷

Communications content is distinguished from non-content and subject to heightened restrictions on disclosure as compared to non-content information. The SCA defines communications “content” as “any information concerning the substance, purport, or meaning of that communication.”³⁸ Content of a stored communication includes both the body of the email and the subject line. Other examples of content include texts, photos and videos; URLs also can be

²⁷ 18 USC § 2703(c)(2).

²⁸ Council of Europe, Convention on Cybercrime, ETS No. 185, November 23, 2001.

²⁹ Art. 18(3) Cybercrime Convention.

³⁰ Art. 1(d) Cybercrime Convention.

³¹ 18 USC § 2703(c)(2).

³² 18 USC § 2510(15); 18 USC § 2711(1).

³³ See, e.g., *In re United States for an Order Pursuant to USC 2705(B)*, 289 F Supp. 3d 201, 203 (DDC 2018) (concluding that Airbnb is an “ECS provider under the SCA by virtue of the electronic messaging system it provides to users of its service”); *Ehling v. Monmouth-Ocean Hosp. Serv.*, 961 F Supp. 2d 659, 667 (DNJ 2013) (holding that Facebook, a social media network, is an electronic service provider); *Warshak v. United States*, 532 F 3d 521, 523 (6th Cir. 2008) (concluding that the statutory definition of an ECS includes basic email services); *Quon v. Arch Wireless Operating Co.*, 529 F 3d 892, 901 (9th Cir. 2008) (holding that a provider of text-messaging pager services is an electronic communications service provider), reviewed on other grounds, *City of Ontario v. Quon*, 560 US 746 (2010).

³⁴ 18 USC § 2711(2).

³⁵ See, e.g., *In re Search Warrant for [Redacted.com]*, 284 F Supp. 3d 970, 974 (CD Cal. 2017) (concluding that a “cloud computing service such as Adobe” is an RCS); *Viacom Intern, Inc. v. YouTube Inc.*, 253 FRD 256, 264 (SDNY 2008) (establishing that YouTube, as an RCS, is prohibited from disclosing “the private videos and the data which reveal their content” that others had uploaded).

³⁶ See, e.g., *Crispin v. Christian Audigier Inc.*, 717 F Supp. 2d 965, 987 (CD Cal. 2010) (concluding that an entity can be both an ECS and an RCS); *In re Search Warrant for Contents of Electronic Mail and for an Order Directing a Provider of Electronic Communication Services to Not Disclose the Existence of the Search Warrant*, 665 F Supp. 2d 1210, 1214 (D Or. 2009) (“Today, most [internet service providers] provide both ECS and RCS.”).

³⁷ See, e.g., *In re United States for an Order Pursuant to 211* (concluding that “an entity that provides ECS or RCS as only one part of its business is still covered by the SCA” and citing cases).

³⁸ 18 USC § 2510(8) and § 2711(1).

content if they contain a search term.³⁹ Some courts have concluded that non-content information can be deemed content if it reveals the substance of a communication.⁴⁰ Only a “governmental entity” – defined as a US department or agency – is given the authority to compel communications content from a covered provider; a combination of SCA rules and the Fourth Amendment requirements leads to the conclusion that the government generally needs a warrant to do so.⁴¹

Under the SCA, non-content data comprises two categories of data – basic subscriber information and all other records that do not rise to the level of communications content. The category of basic subscriber information includes the following: name; address; local and long distance telephone connection records or other records of session time and duration; length of service and types of service used; telephone number or other subscriber number or identity, including a temporarily assigned network address; and means and source of payment.⁴² A US governmental entity can require a provider to disclose basic subscriber information pursuant to an administrative, grand jury or trial subpoena without giving notice to the subscriber or customer.⁴³ Providers can move to quash subpoenas issued under the SCA “if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.”⁴⁴

The second category of non-content data under the SCA includes “record[s] or other information” – meaning the set of non-content data that is not otherwise covered within the category of basic subscriber information.⁴⁵ Some non-content data now comes within the scope of the Fourth Amendment protections announced in *Carpenter v. United States*, discussed in Section 21.2, where the court held specifically that location data spanning more than seven days required a warrant based upon probable cause. For non-content data not covered by *Carpenter*, a US governmental entity must obtain a court order based on “specific and articulable facts” showing that the records sought are “relevant and material to an ongoing criminal

³⁹ See *In re Application of the US for an Order Authorizing Use of a Pen Register*, 396 F Supp. 2d 45, 49 (D Mass. 2005) (concluding that a search phrase within a URL is content); Orin S. Kerr, “A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It” (2004) 72 *George Washington Law Review* 1208, 1228 (explaining the distinction between content and non-content under the SCA: the body and the subject line of an email are content, but logs of account usage, mail header information that does not include the subject line, lists of outgoing email addresses and basic subscriber information, including IP address, are not).

⁴⁰ See, e.g., *In re Google Cookie Placement Consumer Privacy Litig.*, 806 F 3d 137, 137 (3d Cir. 2015) (“In essence, addresses, phone numbers, and URLs may be dialing, routing, addressing, or signaling information, but only when they are performing such a function. If an address, phone number, or URL is instead part of the substantive information conveyed to the recipient, then by definition it is content.”).

⁴¹ Whereas the SCA provides that a US governmental entity can compel ECS providers to disclose emails stored for 180 days or more and RCS providers, regardless of the length of storage, to disclose content pursuant to subpoena and an alternative form of court order, the US Supreme Court decision in *Carpenter v. United States* establishes that, as a matter of constitutional law, a search warrant is required if providers are compelled to disclose communications content, regardless of how long the data has been held. 18 USC § 2703(b); 138 S Ct 2206, 2221 (2018).

⁴² 18 USC § 2703(c)(2). European readers will rightly observe that the notion of “basic subscriber information” under the SCA is broader than the definition of subscriber information or data under European law, which does not include connection records or a temporarily assigned network address (i.e., a dynamic IP address). See Art. 18(3) Cybercrime Convention. See also the definition given by Art. 3(9) of Regulation (EU) 2023/1543 of the European Parliament and of the Council of July 12, 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191/118 (e-Evidence Regulation).

⁴³ 18 USC § 2703(c)(2). Administrative subpoenas permit agencies to compel testimony or the production of documents during investigations or hearings. Similarly, prosecutors use grand jury subpoenas to compel testimony and the production of documents for a grand jury to determine whether certain criminal charges should be brought against an individual. Trial subpoenas permit a court to compel the testimony or production of documents in a criminal proceeding.

⁴⁴ 18 USC § 2703(d).

⁴⁵ From a European perspective, these types of data usually fall under the category of traffic data and location data, also referred to as “metadata.”

investigation.”⁴⁶ Unlike the Wiretap Act, presented in Section 21.3.2, the SCA does not contain any limitations in terms of offenses.

The statute also generally prohibits the voluntary disclosure of stored wire and electronic communications. Specifically, it states that a covered service provider “shall not divulge” stored data to “any person or entity,” unless pursuant to a specified statutory exception, including the kinds of compelled disclosure orders specified by statute.⁴⁷ As already stated, these disclosure provisions differ for content and non-content information – in terms of both what substantive and procedural standards are required in order for the government to compel disclosure and when and under what circumstances providers can disclose data in the absence of a US government-issued order. The rules also differ with respect to whether, in what circumstances and in accordance with what process US-based providers can, consistent with US law, disclose data to foreign governments. Whereas non-content information can be voluntarily disclosed by service providers to foreign government law official agents, content data cannot, absent an executive agreement between the United States and the foreign government, and even then subject to a number of very specific restrictions and criteria (see Section 21.4).

The statute also addresses the issue of notice to the person (or persons) whose data is being collected – incorporating different rules on notice depending on what kind of data is being accessed and according to what process. Government notice to the person whose data is being collected is not required if the government proceeds by warrant or subpoena. It is, however, required if the government proceeds by the kind of court order required for non-content data that is not covered by the definition of basic subscriber information. Even in such situations, the government can delay notification for renewable periods of ninety days if there is a finding that notice will produce an “adverse result” – a category that includes anything that would “seriously jeopardiz[e] an investigation or unduly delay[] a trial.”⁴⁸

In general, providers are given free rein to disclose (or not) governmental requests for data. That said, the government can obtain a gag order to also preclude the provider from disclosing the fact of the compelled disclosure order.⁴⁹ The basis for the issuance of such gag orders is the same as that which enables the government itself to delay notification to the person whose data is being.⁵⁰

If and when evidence is used in a criminal case – if not before – the defendant will be provided governmental notice of the law enforcement action, and evidence obtained, as part of the criminal case. This will generally take place during the pre-trial stage, as part of what is known as the discovery process, in which the defense is entitled to certain information held and relied on by the prosecution.

21.3.2 *The Wiretap Act*

The Wiretap Act (18 USC § 2511 *et seq.*) governs the interception of communications content (as compared to the collection of stored communications content).⁵¹ Content is defined in the same way as it is in the SCA.

⁴⁶ 18 USC § 2703(d).

⁴⁷ 18 USC § 2702(a).

⁴⁸ 18 USC § 2705(a).

⁴⁹ 18 USC § 2705(b).

⁵⁰ In the context of preservation requests, the SCA does not apply, and therefore the decision whether or not to disclose preservation, and at what stage, is entirely up to providers. In practice, providers do not notify users of preservation requests. See Kerr, “The Fourth Amendment Limits,” 776–777.

⁵¹ Any conversation, either over the phone or in person, or any electronic communication that has not yet been received by the recipient, falls within the Wiretap Act. *A contrario*, a communication which is not in transit but instead has already been received and/or stored by the recipient will fall under the scope of the SCA. Therefore, the criteria

Wiretaps are authorized only with respect to certain types of criminal investigation. Initially containing just a few, the list of offenses that can trigger application of a wiretap has grown significantly over the years.⁵²

The process for obtaining a wiretap is more stringent than for stored communications content – or any other search governed by the Fourth Amendment in the absence of additional statutory protections. The judge issuing the wiretap warrant must determine, among other things, that there is probable cause that the particular communications obtained will be about the crime being investigated and that “normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.”⁵³ Wiretaps can only be authorized at thirty-day intervals. Minimization procedures are required, so as to limit the collection of communications “not otherwise subject to interception.”⁵⁴ Court oversight continues even after the period of wiretapping has been completed, requiring that wiretap recordings be “made available to the judge issuing such order and sealed under his directions,” retained in a location ordered by the judge and retained for ten years, among other things.⁵⁵ Notice to the target of the investigation also is required within ninety days of the wiretapping having been completed, but can be postponed after a “showing of good cause” (e.g., if notice would interfere with an ongoing investigation).⁵⁶ Notably, the Wiretap Act is one of the few areas where Congress has set specific limitations on the use of collected information, detailing a specific and exhaustive ground for disclosing such information to others.⁵⁷

The Wiretap Act also includes several mandatory accountability and transparency requirements. According to the latest available report, some 2,245 wiretaps were authorized in 2021, with 1,102 authorized by federal judges and 1,143 by state judges.⁵⁸ Average length of interception was forty-four days. A total of 94 percent of all authorized wiretaps were reported to have used portable devices, including cell phone communications, text messages and application software (apps).⁵⁹

21.3.3 *The Pen Register and Trap and Trace Statute*

The so-called Pen Register and Trap and Trace statute (PRTT) (18 USC § 3121 *et seq.*) governs law enforcement access to dialing, routing, addressing and signaling (DRAS) information utilized in the processing and transmitting of wire or electronic communications – all defined as “non-content” information under US law. Examples include things like incoming and outgoing email addresses,⁶⁰ as well as phone numbers dialed and received.⁶¹ A court order for

determining which regime applies – the SCA or the Wiretap Act – depend on whether the electronic communication sought is in storage or in transit (i.e., in transmission or, in the Cybercrime Convention’s terms, “in real-time”). See Kaitlin G. Klamann, “Show Me the Warrant: Protection of Stored Electronic Communications in New York State” (2014) 41 *Fordham Urban Law Journal* 1407, 1416–1422.

⁵² The list of so-called predicate acts is at 18 USC § 2516(1).

⁵³ 18 USC § 2518(3)(c).

⁵⁴ 18 USC § 2518(5).

⁵⁵ 18 USC § 2518(3)(c).

⁵⁶ 18 USC § 2518(8)(a)–(d).

⁵⁷ 18 USC § 2517(1) specifies that any investigative or law enforcement officer “may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.”

⁵⁸ Wiretap Report 2021, United States Courts, December 31, 2021, www.uscourts.gov/statistics-reports/wiretap-report-2021.

⁵⁹ Wiretap Report 2021.

⁶⁰ So-called DRAS information includes the entire email header except for the “subject” line, which is considered content. See Peter Swire, Justin Hemmings and Suzanne Vergnolle, “A Mutual Legal Assistance Case Study: The United States and France” (2017) 34 *Wisconsin International Law Journal* 334.

⁶¹ 18 USC § 3127(3)–(4) (defining “pen register” and “trap and trace device”).

PRTT can be continuous for a defined period of time, such as all new phone numbers dialed and received, rather than applying only to previously stored information about communications.

Applications for pen registers and trap and trace devices require an application made under oath that the information is “relevant” to an ongoing criminal investigation. Any resulting court order is then served on the relevant provider to implement the pen register or trap and trace; PRTT orders can be authorized for renewable periods of up to sixty days. Notice is precluded unless authorized by the court.

21.3.4 *The Communications for Assistance to Law Enforcement Act*

Both the Wiretap Act and PRTT are coupled with the separate, later enacted CALEA,⁶² which effectively requires telecommunications companies to design and maintain their systems in ways that enable them to assist with either wiretap or PRTT orders. The technical design must ensure that users are not tipped off as to the governmental surveillance.⁶³ Over time, broadband internet access providers and certain providers of voice over internet protocol (VoIP) services have been defined to fall within the definition of “telecommunications carriers” and must meet the requirements of CALEA.⁶⁴

No similar assistance requirement applies with respect to providers of email and digital messaging services (such as Microsoft, Google, Apple, WhatsApp), social media and other hosting service providers (such as Flickr, Instagram), currency exchange services and a range of other providers that arguably have data of interest to law enforcement.

That said, the Act explicitly states that the providers are not responsible for decrypting or ensuring the ability to decrypt such communications.⁶⁵ The result is that communications may be technically intercepted but remain indecipherable because they are encrypted.⁶⁶

The government has separately sought to rely on the All Writs Act – authorizing courts to issue supplemental orders to enforce orders already obtained by the government – to seek to compel technical assistance in those cases in which CALEA is not applicable.⁶⁷ This was the statute relied on in the Apple iPhone case, in which the US government sought technical assistance from Apple in unlocking a phone after the government obtained a warrant to search the phone. The phone had been set to wipe all of its data after ten failed guesses at the password. The government wanted Apple to override this feature so that it could continuously guess the possible passwords until it got it right. The court never resolved the issue because the government found an alternative means (via assistance of a vendor) to access the sought-after data.⁶⁸

Questions about whether and to what extent telecommunication providers, social media companies, providers of digital messaging services, smart phone operating systems and others

⁶² 47 USC § 1001 *et seq.*

⁶³ 47 USC § 1002(a)(b)(4).

⁶⁴ See Federal Communications Commission, “Communications Assistance for Law Enforcement Act and Broadband Access and Services,” First Report and Order and Further Notice of Proposed Rulemaking, August 5, 2005, ET Doc. No. 04-295, www.fcc.gov/document/communications-assistance-law-enforcement-act-calea-and-broadband.

⁶⁵ 47 USC § 1002(b)(3).

⁶⁶ In 2021, encryption was encountered in 176 state wiretaps. In 171 of these wiretaps, officials were unable to decipher the plaintext of the messages. Out of the 183 federal wiretaps that were reported as being encrypted, 161 could not be decrypted. See Wiretap Report 2021.

⁶⁷ 28 USC § 1651.

⁶⁸ Laurie Segall, Jose Pagliery and Jackie Wattles, “FBI Says It Has Cracked Terrorist’s iPhone Without Apple’s Help,” CNN, March 29, 2016, <https://money.cnn.com/2016/03/28/news/companies/fbi-apple-iphone-case-cracked/index.html>.

should be subject to decryption mandates are also the subject of ongoing discussion and debate. To date, there is no explicit authority that permits the government to demand decryption of electronic and wire data.⁶⁹ Nevertheless, US government officials continue to push for such a mandate, given stated concerns about “growing dark” and “warrant-proof encryption” – referring to the inability to access critical evidence needed for criminal cases and general intelligence operations even with a warrant or court order.⁷⁰ Warrant-proof encryption has been of particular concern in child exploitation cases.⁷¹ Still, many others are pushing back, warning of the security and privacy risks associated with any such mandate. A very thoughtful working group report produced by the Carnegie Endowment of International Peace and composed of former government officials, business leaders, computer scientists, law enforcement experts and members of civil society attempted to work through some of the complexities and break through some of the impasse. Recognizing the value of encryption and the risks of unintended consequences, it suggested breaking down the issues and focusing the discussion on what it deemed the “easiest of cases” – namely, access to data at rest on mobile phones – avoiding, at least for now, any sort of regulatory or legislative initiative dealing with the more complex issues associated with data in motion or cloud storage.⁷²

21.4 FOREIGN COOPERATION/DATA ABROAD

There are two distinct issues regarding law enforcement access to data abroad. The first is the issue of US access to data that is located outside the territory of the United States; the second is the issue of foreign access to US-held data.

21.4.1 US Access to Data Held Overseas

Up until the Second Circuit’s 2016 decision in the *Microsoft Ireland* case,⁷³ the United States government generally operated under the assumption that it could compel US-based providers to disclose data in their possession, custody or control without regard to location of the data. Microsoft, however, challenged that assumption – explicitly raising the question of whether a US warrant, issued pursuant to the SCA, could compel disclosure of emails and communications content that are accessed and controlled by a US-based company (Microsoft), but stored on a data server located outside the United States (in Ireland). The Second Circuit Court of Appeals ruled in favor of Microsoft, and concluded that US warrant authority did not extend to data

⁶⁹ The bill on the Lawful Access to Encrypted Data Act was introduced on June 23, 2020 during the 116th session of Congress but did not receive a vote. The bill required certain technology companies to ensure that they can decode encrypted information on their services and products in order to provide such information to law enforcement. S. 4051 – 116th Congress: Lawful Access to Encrypted Data Act. For a fiercely critical analysis, see Riana Pfefferkorn, “There’s Now an Even Worse Anti-Encryption Bill Than Earn It: That Doesn’t Make the Earn It Bill OK,” Center for Internet and Society, Stanford Law School, June 24, 2020, <https://cyberlaw.stanford.edu/blog/2020/06/there-s-now-even-worse-anti-encryption-bill-earn-it-doesn-t-make-earn-it-bill-ok>.

⁷⁰ The Department of Justice has long been concerned about the issue of lawful access to encrypted data. See US Department of Justice, “Lawful Access,” www.justice.gov/olp/lawful-access.

⁷¹ In 2019, the Department of Justice hosted a summit on this topic. See US Department of Justice, “Lawless Spaces: Warrant-Proof Encryption and Its Impact on Child Exploitation Cases,” October 4, 2019, www.justice.gov/olp/lawless-spaces-warrant-proof-encryption-and-its-impact-child-exploitation-cases.

⁷² See Encryption Working Group, *Moving the Encryption Policy Conversation Forward* (Washington, DC: Carnegie Endowment for International Peace, 2019), https://carnegieendowment.org/files/EWG_Encryption_Policy.pdf.

⁷³ *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp. v. United States*, 829 F 3d 197 (2d Cir. 2016).

stored abroad.⁷⁴ However, the Second Circuit’s opinion was binding only in the three US states (New York, Connecticut and Vermont) over which it has jurisdiction. Multiple lower courts in other jurisdictions presented with similar fact patterns disagreed with the Second Circuit Court of Appeals’ ruling,⁷⁵ and the US government appealed its ruling to the US Supreme Court.

The Supreme Court case, however, was mooted when the US Congress resolved the core issue with the March 23, 2018 passage of the CLOUD Act.⁷⁶ Pursuant to this Act,⁷⁷ the government has the explicit authority to access, via a warrant or other form of compulsory process, data from a US-based provider (or, rather, a provider that is subject to US jurisdiction)⁷⁸ of ECS or RCS, provided that the data is within the provider’s “possession, custody, or control,” regardless of the location of the data. When the data is within the provider’s possession, custody or control is not defined by the CLOUD Act, despite it being “the determining factor for whether the service provider must provide the specified evidence.”⁷⁹ However, this concept is well-known in US case law.⁸⁰

Congress also confirmed, via what is known as a “savings clause,” the availability of so-called common law comity claims in the broader set of circumstances in which a conflict of law arises and the statutory provision does not apply. This is something that was available both before and after the CLOUD Act’s enactment and is thus an explicit confirmation of the continuation of the status quo.⁸¹ As far as is known, no such claims of conflict in response to the issuance of US warrants have yet been raised as at the time of writing.⁸² In fact, even in the *Microsoft Ireland* case, neither Microsoft nor Ireland asserted a direct conflict of law. In its amicus brief to the Supreme Court, Ireland emphasized that it was willing and ready to respond to a mutual legal

⁷⁴ Ibid., 222.

⁷⁵ See, e.g., *In re Search Warrant to Google, Inc.*, 264 F Supp. 3d 1268, 1280 (ND Ala. 2017); *In re Search Warrant No. 16-960-M-1 to Google*, 275 F Supp. 3d 605, 619 (ED Pa. 2017), *affg* 232 F Supp. 3d 708 (ED Pa. 2017); *In re Search of Content Stored at Premises Controlled by Google Inc.*, No. 16-mc-80263, 2017 WL 3478809, at *5 (ND Cal. August 14, 2017), *affg* 2017 WL 1487625 (ND Cal. April 25, 2017); *In re Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc.*, No. 16-mj-757, 2017 WL 3445634, at *27 (DDC July 31, 2017), *affg* 2017 WL 2480752 (DDC June 2, 2017); *In re Search of Info. Associated with Accounts Identified as [redacted]@gmail.com*, 268 F Supp. 3d 1060, 1070–1071 (CD Cal. 2017); *In re Search Warrant to Google, Inc.*, No. 16-4116, 2017 WL 2985391, at *12 (DNJ July 10, 2017); *In re Two Email Accounts Stored at Google, Inc.*, No. 17-M-1235, 2017 WL 2838156, at *4 (ED Wis. June 30, 2017); *In re Search of Premises Located at [Redacted]@yahoo.com*, No. 17-mj-1238, slip op. at 3 (MD Fla. April 7, 2017); see also Jennifer Daskal, “Border and Bits” (2018) 71 *Vanderbilt Law Review* 179, 190 (making this point).

⁷⁶ HR 1625, 115th Cong. div. V (2018) (enacted), codified in scattered sections of 18 USC; see *United States v. Microsoft Corp.*, 138 S Ct 1186, 1188 (2018) (per curiam) (ordering that the case be dismissed after finding “[n]o live dispute” between the parties after the passage of the CLOUD Act).

⁷⁷ See also Peter Swire and Jennifer Daskal, “Frequently Asked Questions About the U.S. CLOUD Act,” Cross Border Data Forum, April 16, 2019, www.crossborderdataforum.org/frequently-asked-questions-about-the-u-s-cloud-act/.

⁷⁸ To be subject to US jurisdiction means that US courts exercise personal jurisdiction over the provider in accordance with the Federal Rules of Civil and Criminal Procedure and can thus compel it to produce documents or data. This will obviously be the case for providers that have their headquarters in the US, but also for providers with a subsidiary or business entity in the US. For further analysis and case law examples, see Justin Hemmings, Sreenidhi Srinivasan and Peter Swire, “Defining the Scope of ‘Possession, Custody, or Control’ for Privacy Issues and the CLOUD Act” (2020) 10 *Journal of National Security Law & Policy* 631, 637 ff.

⁷⁹ Ibid., 632.

⁸⁰ For further analysis, see *ibid.*, 654–666.

⁸¹ CLOUD Act § 103(c) (statutory note to 18 USC § 2703).

⁸² The absence of any such conflicts to date undercuts the description of the CLOUD Act as representing a massive expansion of US law enforcement reach and the prediction of increased legal conflict that some suggested would result from allowing US access to data located abroad. See, e.g., Brief for Microsoft Corp., *United States v. Microsoft Corp.*, 138 S Ct 1186 (2018) (No. 17-2), www.supremecourt.gov/DocketPDF/17/17-2/27619/2018011205746909_Brief%20for%20Respondent%202018.01.11.pdf, at 13 (warning of “direct conflicts with foreign laws that govern emails stored in foreign lands”) and at 41.

assistance request for the sought-after data. But it never actually asserted that Microsoft would violate Irish law if it were compelled to disclose the data.⁸³ Such conflicts may nonetheless emerge over time, given, in particular, transfer restrictions included in the EU's General Data Protection Regulation (GDPR)⁸⁴ and the conditions imposed by the case law of the Court of Justice of the EU in relation to transfers of personal data from the EU to the United States.⁸⁵

Notably, this part of the Act *merely* covers providers that are *already* subject to US jurisdiction, clarifying their obligation to disclose data within their possession, custody or control. It is indeed important to emphasize – especially in light of certain concerns expressed by foreign governments⁸⁶ – that the CLOUD Act does not grant the United States any *new* authority to compel disclosure from providers not independently subject to US jurisdiction.⁸⁷ Under current US law, the US warrant authority is territorially limited; hence, there is no applicable authority – either before or after the CLOUD Act – that would authorize US law enforcement to serve a warrant on an extraterritorially located provider.⁸⁸ That said, data held by a foreign-based provider could be accessible to US authorities through a US subsidiary or business entity *if* the latter has “possession, custody, or control” of the data.⁸⁹

In addition to preserving the common law comity claims, the CLOUD Act also includes a new comity provision – out of recognition that requests for data held overseas could, in certain circumstances, generate a conflict of laws. Specifically, it creates a new statutory basis for providers to move to quash based on a conflict with foreign law, albeit only in those limited circumstances in which the conflict is with a “qualifying foreign government” and the United States seeks the data of a non-US person located outside the United States.⁹⁰ To become a qualifying foreign government, the government must have entered into an executive agreement with the United States, pursuant to a number of preconditions, as discussed in Section 21.4.2.

⁸³ Brief for Ireland as Amicus Curiae in Support of Neither Party, *United States v. Microsoft Corp.*, 138 S Ct 1186 (2018) (No. 17-2), www.supremecourt.gov/DocketPDF/17/17-2/23732/20171213152516784_17-2%20ac%20Ireland%20supporting%20neither%20party.pdf.

⁸⁴ See Regulation (EU) 2016/679 of the European Parliament and of the Council, [2016] OJ L 119, May 4, 2016, 1 (GDPR), Arts. 48–49 (laying out transfer restrictions plus exceptions). Whether, to what extent and in what situations the exceptions to the otherwise applicable transfer restrictions will permit a provider to transfer EU-held data to US law enforcement remains an open question. Brief for Microsoft Corp., pp. 13 and 41. On the topic of the GDPR acting as a “blocking statute,” see Jessica Shurson, “Data Protection and Law Enforcement Access to Digital Evidence: Resolving the Reciprocal Conflicts between EU and US Law” (2020) 28 *International Journal of Law and Information Technology* 167.

⁸⁵ See Case 362/14, *Maximillian Schrems v. Data Protection Commissioner* [2015] ECLI:EU:C:2015:650; Case 311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* [2020] ECLI:EU:C:2020:559. See, e.g., Theodore Christakis, “After Schrems II: Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe,” *European Law Blog*, July 21, 2020, <https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/>; Maria H. Murphy, “Assessing the Implications of Schrems II for EU-US Data Flow” (2022) 71 *International and Comparative Law Quarterly* 245.

⁸⁶ Hemmings, Srinivasan and Swire, “Defining the Scope,” 632.

⁸⁷ *Ibid.*, 636–637, 642–643 and 652–653.

⁸⁸ Jennifer Daskal, “Setting the Record Straight: The CLOUD Act and the Reach of Wiretapping Authority under US Law,” *Cross Border Data Forum*, October 1, 2018, www.crossborderdataforum.org/setting-the-record-straight-the-cloud-act-and-the-reach-of-wiretapping-authority-under-us-law.

⁸⁹ See Hemmings, Srinivasan and Swire, “Defining the Scope,” 641–642 (discussing the *Marc Rich* case, concerning a Swiss commodities trading company with a wholly owned subsidiary in the US) and 660–661 (giving the example of a UK entity that hires a US company to handle its data where the latter could have control over the data in certain scenarios).

⁹⁰ CLOUD Act § 103(b), codified at 18 USC § 2703(h). If and when applicable, reviewing courts are instructed to consider the location and the nationality of the investigative target whose data is being sought, the importance of the data to the investigation and the relative interests of the United States and relevant foreign government(s), among other facts.

21.4.2 Foreign Government Access

With this new comity clause, the CLOUD Act responds to the converse problem that foreign governments face with respect to their ability to access communications content held by US service providers. As described in Section 21.3.1, the SCA prohibits US-based providers from disclosing communications content to foreign law enforcement, even if foreign governments are seeking the data of their own nationals in the investigation of local crime. Instead, foreign law enforcement authorities are required to make a government-to-government mutual legal assistance request for such data (often referred to as an MLAT request), even if they are seeking the data of one of their own citizens or residents in connection with a local crime. This is a time-consuming process involving a Department of Justice review of the request, a US Attorney's Office taking the warrant application to a judge on behalf of the foreign government and a subsequent Department of Justice review of any information that is provided before the data is ultimately disclosed to the foreign government.⁹¹ A 2013 report found that it took an average of ten months for the US government to respond to MLAT requests.⁹² While some progress has been made to reform the process in order to enhance the United States' performance in executing incoming MLAT requests, the past years have seen a dramatic increase in such requests, which has slowed response times and strained resources on the United States side.⁹³

Foreign governments are frustrated by this reality, given, in particular, the fact that US-based companies control so much data, including data of foreign citizens and nationals. Paddy McGuinness, the UK's former Deputy National Security Advisor, twice testified before the US Congress about the ways in which the blocking provisions were hampering the UK's ability to investigate and prevent local crime.⁹⁴ At the EU level, Europol reports that delays in the processing of MLAT requests are "a recurring and longstanding challenge for EU authorities."⁹⁵

To address these concerns, Congress authorized the executive branch to enter into agreements with foreign governments, pursuant to which the partner foreign government officials could directly request communications content from US-based providers, subject to specified requirements, without having to employ the mutual legal assistance process. In order to be eligible, the foreign government must first be certified by the Attorney General, in conjunction with the Secretary of State, as "afford[ing] robust substantive and procedural protections for

⁹¹ See Gail Kent, "The Mutual Legal Assistance Problem Explained," *Center for Internet & Society Blog*, February 23, 2015, <http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained> (describing the MLA process).

⁹² See Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein and Peter Swire, *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* (2013), 227, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

⁹³ US Department of Justice, Office of the Inspector General, "Audit of the Criminal Division's Process for Incoming Mutual Legal Assistance Requests," No. 21-097, July 22, 2021, <https://oig.justice.gov/reports/audit-criminal-divisions-process-incoming-mutual-legal-assistance-requests>.

⁹⁴ See Paddy McGuinness, "Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary," June 15, 2017, <https://judiciary.house.gov/wp-content/uploads/2017/06/McGuinness-Testimony.pdf>; Paddy McGuinness, "Hearing Before the S. Judiciary Subcomm. on Crime and Terrorism," May 10, 2017, www.judiciary.senate.gov/imo/media/doc/05-10-17%20McGuinness%20Testimony.pdf; see also Jennifer Daskal, "Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues" (2016) 8 *Journal of National Security & Policy* 473, http://jnslp.com/wp-content/uploads/2017/10/Law-Enforcement-Access-to-Data-Across-Borders_2.pdf.

⁹⁵ Europol, *SIRIUS EU Digital Evidence Situation Report*, 4th Annual Report, December 22, 2022, 47, also 6 and 19. For law enforcement authorities of non-EU countries, the length of the MLA process seems to be an even bigger problem. *Ibid.*, 23.

privacy and civil liberties.”⁹⁶ Each individual request must also meet specified requirements, including those that the requests be particularized, in compliance with the foreign government’s domestic law, based on “articulable and credible facts” and subject to review or oversight by a foreign-government court, judge, magistrate or other independent authority.⁹⁷ Requests must be limited to “serious crimes.”⁹⁸ The CLOUD Act does not define the notion of “serious crime”; it is therefore for each agreement to specify what this threshold entails.⁹⁹

Congress also anticipated the possibility that, pursuant to such agreements, foreign governments could seek live intercepts – and not just stored communications. For live intercepts, the legislation includes the additional requirements that the orders be time-limited, lasting no longer than is needed to accomplish the approved objectives, and subject to a finding that the same information “could not reasonably be obtained by another less intrusive method.”¹⁰⁰

The agreements also include a number of requirements as to the use of collected data. The data must be stored on a “secure system” accessible only to those “trained in applicable procedures.”¹⁰¹ The foreign government is required to segregate, seal or delete non-relevant information.¹⁰² In addition, the foreign government must agree to periodic reviews by the US government to ensure that the provisions of the executive agreement are being followed.¹⁰³

Importantly, the agreements permit partner foreign governments to directly access the data only of non-US persons located outside the United States. Thus, even with an executive agreement in place, partner governments cannot directly compel the production of a US person’s (defined to include US citizens and legal permanent residents)¹⁰⁴ communications content or the communications content of non-US citizens physically located in the United States; these requests still need to go through the mutual legal assistance system.¹⁰⁵ In other words, partner foreign governments can directly access foreigners’ data and hence set the rules, albeit with a number of baseline requirements in place, concerning access to that data. But if the foreign government seeks access to US citizen and resident data, they still need to go through the MLAT process and ultimately get US court approval based on the US standard of probable cause. This stems from the general principle that US standards and procedures should continue to govern access to US citizen and resident data, or persons within the US, but that, so long as baseline human rights conditions are in place, the particular US rules need not govern foreign access to the data of foreigners who are not in the US.

⁹⁶ CLOUD Act § 105(a), codified at 18 USC § 2523 (b)(1).

⁹⁷ CLOUD Act § 105(a), codified at 18 USC § 2523 (b)(4)(D)(ii)–(v).

⁹⁸ For a further elaboration of these protections, see Jennifer Daskal, “Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0” (2018) 71 *Stanford Law Review* 9, 13–15, www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0; Jennifer Daskal and Peter Swire, “Why the CLOUD Act Is Good for Privacy and Human Rights,” *Just Security*, March 14, 2018, www.justsecurity.org/53847/cloud-act-good-privacy-human-rights; Peter Swire and Jennifer Daskal, “What the CLOUD Act Means for Privacy Pros,” *International Association of Privacy Professionals*, March 26, 2018, <https://iapp.org/news/a/what-the-cloud-act-means-for-privacy-pros>.

⁹⁹ Art. 1(14) of the UK–US CLOUD Act Agreement defines serious crime as “an offense that is punishable by a maximum term of imprisonment of at least three years.” It therefore excludes misdemeanors and minor felonies but incorporates a wide range of other crimes. The same threshold is set by the US–Australia CLOUD Act Agreement in its Art. 1(15). For further information on both agreements, see notes 107 and 111.

¹⁰⁰ CLOUD Act § 105(a), codified at 18 USC § 2523 (b)(4)(D)(vi).

¹⁰¹ CLOUD Act § 105(a), codified at 18 USC § 2523 (b)(4)(F).

¹⁰² CLOUD Act § 105(a), codified at 18 USC § 2523 (b)(4)(G).

¹⁰³ CLOUD Act § 105(a), codified at 18 USC § 2523 (b)(4)(J).

¹⁰⁴ CLOUD Act § 105(a), codified at 18 USC § 2523 (a)(2).

¹⁰⁵ CLOUD Act § 105(a), codified at 18 USC § 2523 (b)(4)(A–C).

Finally, the foreign government must provide “reciprocal rights of data access.” This means that the foreign government must permit its own locally based providers to respond directly to US requests for data if and when the United States is seeking the data of a non-national of the partner government, has issued valid legal process to the provider and has jurisdiction to compel such production.¹⁰⁶

The very first agreement between the United States and the UK was agreed to and made publicly available in October 2019.¹⁰⁷ It includes a number of additional provisions above and beyond what is required by the CLOUD Act itself, including a requirement that cross-border requests be reviewed and certified as lawful by a designated authority; explicit procedures by which providers can raise concerns with designated authorities about specific requests; and provisions that require requesting states to notify third-party governments if and when they are requesting the data of someone in that third-party state.¹⁰⁸ The agreement was subject to a (minimum) six-month Congressional review period.¹⁰⁹ Eventually, it entered into force on October 3, 2022.¹¹⁰

A second CLOUD Act agreement between the United States and Australia was reached and made publicly available on December 15, 2021.¹¹¹ The Australian Joint Standing Committee on Treaties gave its approval in December 2022.¹¹²

Furthermore, the United States and Canada entered into formal negotiations in March 2022.¹¹³ As far as a future US–EU agreement is concerned, negotiations began in September 2018, but an agreement has yet to be adopted.¹¹⁴ Stalled negotiations between the EU and the United States can be explained by numerous legal challenges¹¹⁵ and the absence of

¹⁰⁶ CLOUD Act § 105(a), codified at 18 USC § 2523 (b)(4)(I).

¹⁰⁷ Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (UK–US CLOUD Act Agreement), Washington, October 3, 2019, USA No. 6 (2019), CP 178, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

¹⁰⁸ For an analysis of the new and interesting provisions in the UK–US CLOUD Act Agreement, see Jennifer Daskal and Peter Swire, “The UK-US Cloud Act Agreement Is Finally Here, Containing New Safeguards,” Just Security, October 8, 2019, www.justsecurity.org/66507/the-uk-us-cloud-act-agreement-is-finally-here-containing-new-safe-guards/.

¹⁰⁹ There is a 180-day waiting period between the time the agreement is submitted to Congress and the ultimate implementation. During that time, Congress can, via joint resolution, prohibit the agreement from going into effect.

¹¹⁰ US Department of Justice, “Landmark U.S.-UK Data Access Agreement Enters into Force,” October 3, 2022, www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force.

¹¹¹ Agreement between the Government of the United States and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime (U.S.–Australia CLOUD Act Agreement), December 15, 2021, www.justice.gov/dag/page/file/1465616/download; see also Australian Department of Home Affairs, “Australia-US CLOUD Act Agreement,” www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/australia-united-states-cloud-act-agreement.

¹¹² Joint Standing Committee on Treaties, *Report 204. Agreement between the Government of Australia and the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime*, December 2022, https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024997/toc_pdf/Report204.pdf;fileType=application%2Fpdf; Paul Karp, “Green Light for US Law Enforcement to Demand Data from Australian Communication Providers,” *Guardian*, December 26, 2022, www.theguardian.com/australia-news/2022/dec/27/green-light-for-us-law-enforcement-to-demand-data-from-australian-communication-providers.

¹¹³ US Department of Justice, “United States and Canada Welcome Negotiations of a CLOUD Act Agreement,” March 22, 2022, www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement.

¹¹⁴ European Commission, *Joint Statement on the Launch of EU-U.S. Negotiations to Facilitate Access to Electronic Evidence*, September 26, 2019, https://ec.europa.eu/commission/presscorner/api/files/document/print/es/state_ment_19_5890/STATEMENT_19_5890_EN.pdf.

¹¹⁵ See Theodore Christakis and Fabien Terpan, “EU-US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options” (2021) 11 *International Data Privacy Law* 81;

internal EU rules on e-evidence.¹¹⁶ With the adoption of the so-called e-Evidence package¹¹⁷ on January 25, 2023 under the Swedish presidency of the EU Council,¹¹⁸ that important obstacle to US–EU negotiations will soon no longer apply.

21.5 LOOKING FORWARD

The question of access to data across borders remains a fraught and critically important one both for the United States and globally. Data needed in the investigation of even local crimes is increasingly located outside the investigating country's border and much of this data is in the hands of US-based providers. The CLOUD Act is an attempt to address that, but in a piecemeal way.¹¹⁹

The underlying premise is the correct one: It recognizes that the United States should not and need not review every foreign request for US-held data pursuant to the specific US standard of a warrant based on probable cause. Yet, at the same time, it insists on baseline standards and protections that every request for communications content ought to meet. Importantly, these are baseline requirements that set a floor. Individual executive agreements can, and should, add additional specificity to ensure, for example, meaningful independent review of requests, transparency about the number and nature of the requests and an effective mechanism to enable providers to raise concerns if they receive foreign-based requests that appear to fall outside the approved criteria. Meanwhile, further work is needed to address the difficult question of access to data across borders – in ways that establish baseline procedural and substantive protections, no matter who is doing the requesting and where the request is being directed.¹²⁰

The efforts of the Council of Europe to update the Budapest Convention, by the adoption of a Second Additional Protocol,¹²¹ are a start in the right direction. The Second Additional Protocol to the Budapest Convention, which has been signed by the US,¹²² aims at facilitating

Jennifer Daskal and Peter Swire, “A Possible US-EU Agreement on Law Enforcement Access to Data?,” *Lawfare*, May 21, 2018, www.lawfareblog.com/possible-eu-us-agreement-law-enforcement-access-data.

¹¹⁶ Thomas Wahl, “E-Evidence: Start of Negotiations on EU-US Agreement,” *EUCrim*, January 12, 2020, <https://eucrim.eu/news/e-evidence-start-negotiations-eu-us-agreement/>.

¹¹⁷ The “e-Evidence package,” proposed by the European Commission in April 2018, consists of two legal instruments, a Regulation enabling the cross-border production of communications (content and non-content) data in the EU and a Directive requiring EU service providers that are active in more than one EU member state as well as non-EU service providers active in the EU to designate a legal representative for the purpose of gathering electronic evidence in criminal proceedings. For further analysis, see Chapter 7 in this volume.

¹¹⁸ Council of the EU, “Electronic Evidence: Council Confirms Agreement with the European Parliament on New Rules to Improve Cross-Border Access to e-Evidence,” January 25, 2023, www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/.

¹¹⁹ See Daskal, “International Lawmaking 2.0”; Jennifer Daskal, “Unpacking the CLOUD Act,” *EUCrim*, January 31, 2019, <https://doi.org/10.30709/eucrim-2018-022>; Daskal and Swire, “Why the CLOUD Act Is Good”; Swire and Daskal, “What the CLOUD Act Means.”

¹²⁰ As noted by Jennifer Daskal and Debrae Kennedy-Mayo, some states and outside observers, including human rights organizations and service provider associations, have expressed concerns about law enforcement actors being able to compel production of data anywhere under domestic authority alone and the risk of abuse this entails. They argue that the risks can and should be mitigated by, inter alia, use of procedural and substantive protections, transparency and effective mechanisms for accountability. See Jennifer Daskal and Debrae Kennedy-Mayo, “Budapest Convention: What Is It and How Is It Being Updated?,” *Cross-Border Data Forum*, July 2, 2020, www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/#_edn42.

¹²¹ Council of Europe, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, ETS No. 224, Strasbourg, April 12, 2022.

¹²² Deputy Assistant Attorney General Richard Downing of the US Department of Justice’s Criminal Division signed the Additional Protocol on May 12, 2022 on behalf of the US government. See US Department of Justice, “United

mutual legal assistance and allowing direct cooperation with service providers while implementing stronger safeguards for existing practices of transborder access to data.¹²³

Of course, US law can and should evolve as well. The US requirement of a warrant based on probable cause for communications content and other kinds of highly sensitive data is what some have called the “gold standard” – a relatively high form of protection replete with requirements of particularity and independent review. Yet, based on a combination of the third-party doctrine and statutory lacuna, there has long been a range of personal and highly sensitive data that is accessible to law enforcement by standards much laxer than the warrant requirement. The Supreme Court’s decision in *Carpenter* begins to change this. While ostensibly about historical location data alone, the case broadly recognizes that individuals do not, and should not be understood to, lose Fourth Amendment-based privacy protection in all of their data simply because it is in the hands of a third-party provider that manages it. The doctrine is continuing to evolve and the contours of what is and is not protected by the warrant requirement will be worked out for years to come.¹²⁴

There also is a need to focus, both in the United States and elsewhere, beyond the point of acquisition toward questions of use. The Wiretap Act is a model, setting clear limits on retention and dissemination. And the CLOUD Act, too, imposes use limitations, requiring a range of limits on the dissemination, retention and review of acquired data as a precondition of any executive agreement. But outside those two areas,¹²⁵ Congress – and the Fourth Amendment doctrine – has been largely silent on the question of use, focusing most of the analysis and law on the rules governing collection. This should change. Given the potential for vast collection, long-term storage and dissemination of data, there is an urgent need to set broader parameters on the acceptable standards and practices with respect to retention, dissemination and ongoing accessing of collected data. Basic cyber-hygiene issues with respect to secure storage and access systems are critical as well. In the EU, such issues have been addressed by the GDPR, which sets principles and imposes strict conditions for the processing of personal data.¹²⁶ It remains to be seen whether and how these conditions will be reflected in the future EU–US Data Privacy Framework.¹²⁷

States Signs Protocol to Strengthen International Law Enforcement Cooperation to Combat Cybercrime,” www.justice.gov/opa/pr/united-states-signs-protocol-strengthen-international-law-enforcement-cooperation-combat.

¹²³ For further analysis, see Chapter 8 in this volume.

¹²⁴ For an overview of the application of *Carpenter* by federal courts and state courts between June 2018 and March 2021, see Tokson, “The Aftermath of *Carpenter*.”

¹²⁵ In addition, it is worth pointing out the existence of limitations on use, onward transfer and retention of data in the context of cross-border exchange of data between governments and law enforcement agencies. See, e.g., Arts. 6–7 and 12 of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences (“EU–US Data Protection Umbrella Agreement”), [2016] OJ L 336, December 10, 2016, 3.

¹²⁶ See Arts. 5 and 6 of the GDPR, detailing the principles relating to the processing of personal data and laying out the conditions for lawful processing, respectively.

¹²⁷ Unlike the EU–US Data Protection Umbrella Agreement, the EU–US Data Privacy Framework will regulate the transfers of data by *private entities* in the EU to the US, and vice versa. The formal process to adopt an EU–US adequacy decision was launched by the European Commission in December 2022, after President Biden adopted an Executive Order in October 2022. See European Commission, “Questions & Answers: EU–U.S. Data Privacy Framework, Draft Adequacy Decision,” December 13, 2022, https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632; White House, “Executive Order to Implement the European Union–U.S. Data Privacy Agreement,” October 7, 2022, www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.

Conclusion

Collecting Digital Evidence – From Present Challenges to Future Solutions

Vanessa Franssen and Stanisław Tosza

COMMON CHALLENGES, DISPARATE SOLUTIONS

The purpose of this handbook has been to provide an all-encompassing, intra-disciplinary analysis of the challenges relating to the gathering of digital evidence in criminal matters and the solutions that may be found in different legal orders, whether national, supranational or international. The rich analyses offered by the various chapters in this volume have enabled us to get a better understanding of the current problems as well as the solutions that are put forward to address them. If one thing, those analyses confirm that the challenges are highly comparable in all legal systems and for all stakeholders – law enforcement authorities (LEAs), private actors and citizens. Indeed, the collection of digital evidence calls into question the core principles and elements of any criminal justice system, such as sovereignty, territoriality, legal certainty, judicial review and the protection of fundamental (or human) rights.¹ The powers of public authorities are shifting, and so is the role of private actors whose cooperation has become essential to the success of many criminal investigations, for all types of crime.

Nevertheless, even though the challenges are shared, the legal answers are not. The national chapters in this book show that legal solutions to similar problems are disparate, and often unsatisfactory, thereby creating new challenges. This is especially the case when LEAs resort to unilateral measures with extraterritorial reach or collaborate with other states or private actors without a clear legal framework. Moreover, while the challenges are complex and multidimensional, legal solutions are all too often fragmented, focused on specific issues and situations, or developed in a haphazard or casuistic way.

At supranational and international levels, the legal landscape indeed continues to be extremely fragmented. This fragmentation was clear from the outset, as it was one of the starting points of our research. Notwithstanding several positive developments that have taken place since (such as the adoption of the Second Additional Protocol to the Cybercrime Convention,² the e-Evidence Regulation³ at European Union (EU) level and the Organisation for Economic Co-operation and Development (OECD) Guidelines on

¹ For a more in-depth analysis of the impact of digital evidence gathering on the criminal justice system, see Chapter 1 in this volume.

² Council of Europe, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, ETS No. 224, Strasbourg, 12 April 2022 (Second Additional Protocol).

³ Regulation (EU) 2023/154 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings [2023] OJ L 191/118 (e-Evidence Regulation).

Government Access to Data⁴) and the current preparation of other important solutions for cross-border cooperation (such as the Clarifying Lawful Overseas Use of Data (CLOUD) Act Executive Agreement between the United States and the EU), fragmentation will remain a major challenge in the years to come, in particular outside of the intra-EU and EU–US cooperation. To overcome this problem, further international collaboration is indispensable. Yet, political agreements at international level are notoriously hard to reach, and in the digital era fundamental differences in values oppose democratic states to non-democratic states more than ever before. This tension is, for instance, very tangible in the negotiations on the United Nations Cybercrime Treaty.⁵

NEED FOR COMMON TERMINOLOGY

From the national legal systems studied in this handbook, it results clearly that they all struggle with the questions triggered by digitalisation in the context of criminal procedure. For a start, the terminology used is often inadequate. It suffices to zoom in on the notion of ‘digital evidence’, which is commonly used in legal doctrine but inexistent in most codes of criminal procedure; on the definition and categorisation of data; or on the labels given to different kinds of service provider.⁶ One could argue that terminology is only a preliminary step and not nearly as important as the solutions that are offered in substance. But without common terms there is no shared basis for cooperation, whether between states or between public authorities and private actors.

In the EU, the e-Evidence Regulation marks an important step in building a solid legal framework for the purpose of cross-border gathering of digital evidence, including common terms and definitions, just like the Council of Europe Cybercrime Convention did in 2001. These are examples that merit being followed, even if no definition is perfect or exempt from grey zones.⁷

That said, there is still considerable room for improvement at EU level. Contrary to the Cybercrime Convention, EU law is characterised by a variety of terms referring to different types of online service and their providers (e.g. electronic communications services and information society services, which are further subdivided), governed by a jigsaw puzzle of sectoral rules.⁸ Some of these rules are directly related to the field of criminal law, but many are not. This sectoral diversity is confusing and will inevitably lead to new clashes and conflicting legal obligations. Even top-level EU officials seem to struggle to understand which legal framework applies to which service (provider),⁹ and the same goes for big providers with considerable legal

⁴ Organisation for Economic Co-operation and Development (OECD), ‘Declaration on Government Access to Personal Data Held by Private Sector Entities’, 2023, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>.

⁵ For information on the preparations of this treaty, see the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

⁶ See the comparative Chapter 16 in this volume, Section 16.2.

⁷ On the e-Evidence Regulation, see, e.g., V. Franssen, ‘Cross-Border Gathering of Electronic Evidence in the EU: Toward More Direct Cooperation under the e-Evidence Regulation’, in V. Mitsilegas, M. Bergström and T. Quintel (eds.), *Research Handbook on EU Criminal Law*, 2nd ed. (Edward Elgar, 2024), 183–210. On the Cybercrime Convention, see, e.g., J. Clough, ‘The Council of Europe Convention on Cybercrime: Defining “Crime” in a Digital World’ (2021) 23 *Criminal Law Forum* 363.

⁸ For further examples, see Chapter 16 in this volume.

⁹ See, e.g., S. de Biolley, ‘Overview of the (Future) Regulations Applicable to Service Providers’, presentation at an expert workshop (*Evidence-Based Cyberviolence Policy in Europe*) organised by the University of Antwerp in the

resources, especially since online services often entail different features that are not easy to fit into one box. When both regulators and regulated entities experience difficulties in figuring out which legal rules apply to which services, this calls for reflection.

On top of this EU legal imbroglia comes national diversity, which leads to further fragmentation and disparities. Moreover, the terms used in national criminal procedure are not necessarily identical to the ones used in other fields of law which are directly influenced by EU law (e.g. e-commerce, economic law, telecommunications law).

In light of the ‘borderless’ nature of the internet, the fragmented legal landscape is a real concern as it hampers the fight against new criminal phenomena, putting the rights of citizens around the world in danger. What is more, the current patchwork hardly testifies to a ‘technology-neutral’ approach which is so often advocated for by academic and other experts,¹⁰ and thus it is a safe bet that it will not stand the test of time. The EU is, however, not alone in taking this approach. Elsewhere in the world, one may find regulatory approaches that slice up online services in an attempt to put their providers in separate boxes with different legal obligations. The Chinese approach is a telling example.¹¹

IN SEARCH OF COHERENCE

In addition to the patchwork of sectoral legislation, the coherence and the interplay between different EU legal instruments are not always clear. In the criminal justice area, legal scholars have been insisting for many years on the need for consistency and coherence in EU law.¹² While several attempts have been made to create more consistency,¹³ EU legal instruments remain the outcome of topic-specific negotiations which result in disparate solutions for similar or related problems. This also holds true for the rules concerning cross-border evidence gathering. For instance, the e-Evidence Regulation provides for only two cross-border orders – European preservation orders and European production orders. Other orders to service providers remain, in principle, national in scope. This is, for instance, the case for orders to decrypt data or to assist a LEA in performing a search in an information system. With respect to orders to remove illegal content online, the situation is less straightforward. Removal orders concerning online hate speech or child sexual abuse material apply nationally, that is, to national service providers.¹⁴ When addressing a foreign service provider, such orders can only be enforced when issued as European Investigation Orders. Moreover, there is no EU-wide obligation to obey such removal

framework of the @ntidote 2.0 research project, funded by BELSPO (Belgian Science Policy Office), in cooperation with the University of Liège and UCLouvain Saint-Louis Bruxelles, Antwerp, 8–9 December 2022.

¹⁰ See, e.g., Clough, ‘The Council of Europe Convention on Cybercrime’, 375 ff.

¹¹ See Chapter 17 in this volume.

¹² See, e.g., European Criminal Policy Initiative, ‘The Manifesto on European Criminal Policy in 2011’ (2014) 4 *European Criminal Law Review* 86; P. Asp, ‘The Importance of the Principles of Subsidiarity and Coherence in the Development of EU Criminal Law’ (2011) 1 *European Criminal Law Review* 44; V. Franssen, ‘EU Criminal Law and Effet Utile – A Critical Examination of the Use of Criminal Law to Achieve Effective Enforcement’, in J. Banach-Gutierrez and C. Harding (eds.), *EU Criminal Law and Crime Policy: Values, Principles and Methods* (Abingdon: Routledge, 2016), 84–110.

¹³ European Commission, *Towards an EU Criminal Policy: Ensuring the Effective Implementation of EU Policies through Criminal Law*, COM (2011) 573 final, 20 September 2011.

¹⁴ Compare with Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2011] OJ L 325/1, Art. 25(1).

orders.¹⁵ In contrast, in case of terrorist content online, removal orders entail an obligation to remove the content or disable access to it on the entire EU territory.¹⁶ When the service provider hosting terrorist content online does not have its main establishment or legal representative in the member state of the issuing authority, a specific procedure for cross-border enforcement is foreseen in Article 4 of the Terrorist Content Online Regulation. This procedure is, however, not identical to the one set forth by the e-Evidence Regulation. Therefore, LEAs issuing orders to foreign service providers will have to pay careful attention to the legal framework that applies to the order at hand.

CRIMINAL PROCEDURE MEETS DATA PROTECTION

In addition, as highlighted in many chapters of this handbook and explained in an in-depth manner in the chapter dedicated to data protection,¹⁷ the articulation of criminal procedure and data protection rules continues to pose many questions. This is true at EU level, where different rules apply to LEAs when conducting a criminal investigation (the rules laid down in the Law Enforcement Directive (LED))¹⁸ and service providers cooperating with those LEAs (the General Data Protection Regulation (GDPR))¹⁹.²⁰ Yet, the national implementation of the LED further complicates the picture. As other research demonstrates, national implementing laws do not always meet the requirements of the LED.²¹ Some of these laws have already been scrutinised by the Court of Justice of the European Union (CJEU).²² With the entry into force of the e-Evidence Regulation, many new issues are likely to come to the surface. The e-Evidence Regulation will, however, not solve the issue of decryption orders,²³ which may be imposed under national law.

¹⁵ Admittedly, the Digital Services Act imposes obligations on service providers to cooperate with national public authorities, but it does not entail an obligation to act against illegal content following an order issued by a national authority. It obliges service providers only to inform the authority issuing the order or any other authority specified in the order of any follow-up given to the orders, without undue delay, specifying if and when the order was applied. Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services and amending Directive 2000/31/EC of 19 October 2022 (Digital Services Act), [2022] OJ L 277/1, Art. 9(1). See M. Walrave, C. Van de Heyning, V. Franssen, C. Mathys, J. Vrielink, M. Giacometti, A. Gilen and O. Gangi, *Cyberviolence: Defining Borders on Permissibility and Accountability – @ntidote 2.0. Final Report* (Brussels: BELSPO, 2023), 81, www.belspo.be/belspo/brain2-be/projects/FinalReports/Antidote_FinRep_en.pdf.

¹⁶ Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online [2021] OJ L 64/79 (Terrorist Content Online Regulation), Art. 3(1) and (3).

¹⁷ See Chapter 3 in this volume.

¹⁸ Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89 (Law Enforcement Directive (LED)).

¹⁹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 (GDPR).

²⁰ This distinction has been clarified by the CJEU: Case C-623/17, *Privacy International* [2020] ECLI:EU:C:2020:790. For an analysis, see J. Sajfert, 'Bulk Data Interception/Retention Judgments of the CJEU – A Victory and a Defeat for Privacy', *European Law Blog*, 26 October 2020, <https://europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/>.

²¹ E. Kosta and F. Boehm (eds.), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford: Oxford University Press, 2024).

²² See, e.g., Case C-333-22, *Ligue des droits humains ASBL*, 16 November 2023, concerning the right to an effective remedy against the decision of the supervisory authority as provided by Article 17(3) of the LED.

²³ E-Evidence Regulation, Recital 20. For a first analysis, see V. Franssen, 'Cross-Border Gathering of Electronic Evidence in the EU' at 208–209.

UNDER-REGULATED ISSUES

Even if legislators around the world try to regulate the provision of online services and the obligations of their providers, other aspects that are highly relevant for the collection of digital evidence remain under-regulated. Indeed, a number of questions, while clearly identified as concerns for LEAs, have not yet been sufficiently addressed at EU or international levels. Data retention is definitely one of them. While EU law as interpreted by the CJEU is setting clear limits to data retention obligations, especially with respect to traffic and location data (or ‘metadata’), such obligations continue to exist at the national level. Elsewhere in the world, extensive data retention obligations exist (e.g. in China)²⁴ and different solutions have been adopted to get around the problem of access to data (e.g. in the US).²⁵

Whereas the EU legislator has abandoned the location of data as a decisive territorial criterion – at least in the e-Evidence Regulation – the place where data is stored remains an important nexus for determining jurisdiction elsewhere in the world, and even at the level of the Council of Europe.²⁶ Therefore, many legal systems (e.g. China,²⁷ Russia²⁸ and Turkey²⁹) are still inclined to impose data localisation obligations to be able to access data for the purpose of criminal investigations.

Finally, the boundaries between intelligence and criminal law remain notoriously difficult to draw, even if both pursue different objectives and obey distinct legal regimes.³⁰ In practice, though, the walls between intelligence activities and criminal investigations are much less thick. This entails inherent risks for citizens’ fundamental rights. Aware of these risks, the CJEU in its data retention case law draws hard boundaries between data collection for intelligence purposes and the gathering of data for evidence purposes.³¹ At national level, however, the distinction between intelligence activities and criminal investigative measures is often blurred, especially in totalitarian regimes.³²

TOWARDS FUTURE SOLUTIONS

Taking the perspective of citizens affected by law enforcement measures, it is striking that procedural safeguards and legal remedies remain under-regulated, especially in a cross-border setting. No one questions that fundamental rights, such as the right to a fair trial, are also applicable in cross-border situations. But their concrete content tends to diverge greatly across national systems and even at the supranational level. This puts citizens using online services in a very delicate position. For service providers this creates both challenges and opportunities. Some service providers try to fill the void and actively step in to protect their customers’ rights, even if they are reluctant to play the role that public authorities should normally take up. At the same time, the lack of a clear cross-border fundamental rights framework gives service providers leeway to apply their own corporate policies, across legal systems.³³ For sure, some EU legal

²⁴ See Chapter 17 in this volume.

²⁵ See Chapter 21 in this volume.

²⁶ See Chapter 2 in this volume.

²⁷ See Chapter 17 in this volume.

²⁸ See Chapter 18 in this volume.

²⁹ See Chapter 19 in this volume.

³⁰ See Chapter 6 in this volume.

³¹ See, e.g., Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net* [2020] ECLI:EU:C:2020:791, paras. 134–139; Case C-140/20, *G.D. v. Commissioner of An Garda Síochána* [2022] ECLI:EU:C:2022:258, para. 100.

³² See, e.g., Chapter 18 in this volume.

³³ See also S. Tosza, ‘Internet Service Providers as Law Enforcers and Adjudicators: A Public Role of Private Actors’ (2021) 43 *Computer Law & Security Review* 1.

instruments provide for specific procedural safeguards. For instance, the e-Evidence Regulation contains an explicit requirement of an *ex ante* judicial authorisation as far as European production orders for traffic and content data are concerned.³⁴ Elsewhere, only the general requirement of an effective remedy is imposed,³⁵ leaving it up to member state law to define the content of such remedy. The analyses of the seven EU member states in this handbook show that such a general requirement gives rise to very different approaches and uneven protection of citizens' rights.

An ultimate protection of fundamental rights could be found in the rules on admissibility of evidence. Yet, the national analyses in this volume reveal that domestic rules are rather flexible – even more so in a cross-border setting. In practice, illegally obtained evidence is often excluded only in the case of very serious violations of (certain) fundamental rights. This proves the importance of having robust procedural safeguards and sufficient checks and balances during the criminal investigation, rather than relying on *ex post* remedies. At EU level, the CJEU has started to set minimum requirements, too, for the admissibility of evidence, once more in the context of its data retention case law,³⁶ but the concrete impact of these requirements at national level calls for further investigation.

To conclude, the protection of fundamental rights is clearly a weak spot in the collection of digital evidence, especially in a cross-border context. Therefore, policymakers around the world should dedicate all their attention to strengthening those rights, striking a delicate balance between effective protection and efficient criminal investigations.

³⁴ E-Evidence Regulation, Art. 4(2).

³⁵ See, e.g., e-Evidence Regulation, Art. 18.

³⁶ *La Quadrature du Net*, paras. 221–228.