D2.1

Fundamental support study on encryption and fundamental rights

Project number:	883156
Project acronym:	EXFILES
Project title:	Extract Forensic Information for LEAs from Encrypted SmartPhones
Start date of the project:	1st July, 2020
Duration:	36 months
Programme / Topic:	H2020-SU-SEC-2019 / SU-FCT02-2018-2019-2020 Technologies to enhance the fight against crime and terrorism

Deliverable type:	Report
Deliverable reference number:	SU-FCT02-883156 / D2.1/ V1.0
Work package contributing to the deliverable:	WP2
Due date:	Dec 2021 – M18
Actual submission date:	4th February, 2022

Responsible organisation:	ULille
Editor:	Audrey Dequesnes
Dissemination level:	PU
Revision:	1.0

Abstract:	This deliverable is the first legal analysis of the EXFILES project. It is the result of the study of numerous national and European documents from various sources - institutional, academic, legal, technical, law enforcement, and NGO - as well as contributions from the project partners on the legal framework applicable in their country. It assesses the legal and soft-law provisions regarding fundamental rights and the use of encryption, in the context of collection of evidence from encrypted devices.
Keywords:	Fundamental rights, privacy, encryption, forensic methods, legal framework, digital evidence, European Union's law, Council of Europe.

The project EXFILES has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883156.

Editor

Audrey Dequesnes (ULille)

Contributors (ordered according to beneficiary numbers)

Laurène Baudouin, Clara Debruyne, Audrey Dequesnes, Tilila Lanux, Sébastien Leleu, Marcel Moritz, Serlin Serap, (ULille)

IRCGN

BKA

CNI

NFI

RHUL

NCIS

Disclaimer

Executive Summary

This deliverable is the first legal analysis of the EXFILES project. It is the result of the study of numerous national and European documents from various sources - institutional, academic, legal technical, law enforcement, and NGO - as well as contributions from the project partners on the legal framework applicable in their country.

It provides a broad overview of the legal framework applicable to digital investigations and digital forensics at the international level, from the Council of Europe, the European Union and the Member States participating in the project. This framework is further analysed along the lines of the fundamental rights that may be impacted by the decryption and recovery of digital evidence, the processing of such evidence, and finally the handling of the resulting data and the police files. These rights are mainly the right to privacy and protection of personal data, the right against self-incrimination, the right to a fair trial and the proportionality of the infringement of these rights. In some of the participant countries in this project, legal provisions exist for the seizure, retrieval and handling of electronic evidence, or specific to encryption, which may include sanctions for its use.

Given the challenges arising from encryption, the cooperation of service providers would often be required to carry out investigations, and cases where this is covered by a legal provision will be studied. In cases where this cooperation does not take place, either for technical reasons or because of unwillingness, the methods used by law enforcement agencies to achieve decryption are given legal protection.

Although criminal investigations are a prerogative of the States, data exchange and cooperation are of primary importance to these activities, therefore the framework for this cooperation is also examined.

Table of Content

Chapter 1 Introduction 1

Chapter 2 Overview of the international legal framework and main stakeholders ..8

2.1 The United Nations provisions 9

2.1.1 United Nations' International Covenant on Civil and Political Rights 10

2.1.2 United Nation's Convention against Transnational Organise Crime 11

2.1.3 Interpol 13

2.2 The founding contributions of the Council of Europe 14

2.2.2 European Convention on Human Rights and Fundamental Freedoms 15

2.2.3 The Convention on Cybercrime 15

2.2.4 The Convention on Mutual Assistance in Criminal Matters, and its additional protocols. 20

2.2.5 Stakeholders 23

Chapter 3 Encryption, e-evidence and fundamental rights 25

3.1 Legality of offences 25

3.2 Respect for privacy 25

3.2.1 European framework 25

3.2.2 National legal frameworks 27

3.2.3 Focus on the necessary safeguards regarding the mass interception of communications 35

3.2.4 National restrictions on the use of encryption 36

3.3 Proportionality 38

3.4 Subsidiarity 38

3.5 Right not to self-incriminate 39

3.5.1 European framework 40

3.5.2 National frameworks 42

3.5.3 Perspectives and recommendations 46

3.6 Right to a fair trial 46

3.6.1 The right to evidence 47

3.6.2 The right to defence 47

Chapter 4 Legal challenges of investigation and evidence 50

4.1 Seizure, interception, copy, write block 50

4.2 Mining, extraction 51

4.3 Integrity of evidence 52

4.3.1 The European framework for the integrity of digital evidence 52

4.3.2 National frameworks for the integrity of evidence 53

4.3.3 Reliability of the technique used and integrity of evidence 54
4.4 Retrieving of unencrypted data 55
4.4.1 Direct extraction 56
4.4.2 Legal protection of methods used by law enforcement 59
4.4.3 Remote access on the cloud 59
4.5 National procedures in obtaining digital evidence 60
4.5.1 The Encrochat case 60
4.5.2 National procedures 62
4.6 Distinction between preventive and investigative measures 64
4.7 Cooperation between investigative services 67
4.7.1 Data exchange and cross-border investigation 68
Chapter 5 Data protection 72
5.1 The EU legal framework on personal data protection 72
5.1.1 Scope of the Law Enforcement Directive 72
5.1.2 The principles of data protection with LED 74
5.1.3 Transfers of personal data to a third country 78
5.1.4 The challenges of transposing the LED 79
5.2 Police and judicial files 81
5.2.1 National police files: the case of France 82
5.2.2 At the international level 85
5.2.3 The Schengen Information System 87
5.2.4 The SIRIUS platform 88
5.3 Type of data collected 90
5.3.1 Non-content data 90
5.3.2 Content data 94
5.3.3 Cross-referencing of personal data 96
5.4 Data retention 96
5.4.1 Retention of data by telecommunication operators 96
5.4.2 Duty of cooperation of telecommunication operators 101
5.4.3 Retention of other types of data 107
5.4.4 Remarks on ePrivacy regulation and law enforcement 107
5.4.5 Perspectives and recommendations 108
Chapter 6 Summary and Conclusion 109
Chapter 7 List of Abbreviations 110
Chapter 8 Bibliography 113

List of Figures

Figure 1: Example of end-to-end encryption..... 1
Figure 2: Areas covered by the Budapest Convention. 17

List of Tables

Table 1: National frameworks for secrecy correspondence 28
Table 2: Possible sanctions for using encryption..... 36
Table 3: Legal obligation for individuals to decrypt 43
Table 4: Data decryption procedure 56
Table 5: Obligation of telecommunications service providers to assist the authorities 101

Chapter 1 Introduction

Digital innovation has turned the world into a society entirely based on information systems where individuals are dependent on the overall security of these information systems. The use of new technologies and the Internet facilitates numerous activities such as communication, healthcare and working conditions, but it also introduces new risks and constraints. For instance, the protection of anonymity in the digital domain allows a great deal of freedom, sometimes in access and often misused and therefore needs to be regulated. This situation has encouraged the development of cybercrime (i.e. the commission of offences via the Internet). The universality of the Internet, its accessibility, and the freedom and neutrality that it promotes has offered the possibility for crime to express itself in new ways through it.

Cybersecurity has become a key global issue because it is through it that acts of cybercrime are anticipated and repressed. Today, cybercrime is no longer limited to isolated initiatives, it has professionalized itself and affects many areas such as espionage, or economic intelligence. Cybercrime doesn't need a state-of-the-art equipment: simple cellphones or smartphones (tools of everyday life) are sufficient. Recent studies estimate that 4.3 billion people will be smartphone users by 2023[1]. The fight against cybercrime has become a very complex legal issue that aims at preventing and punishing cybercrime. In addition to maintaining security and law enforcement in the physical world, law enforcement agencies have seen their prerogatives extended to the cyber domain. This fight requires a great deal of legal, organisational, procedural, technical and human resources, as it is difficult to maintain a high level of efficiency with the pace of technological change. Indeed, technology develops very quickly and it is difficult to anticipate its evolution in order to implement new adequate means to its management.

There are many tools available to everyone that are designed to protect communications. Encryption, for instance, is one of the most efficient and common tools used to provide a secure environment for communications.

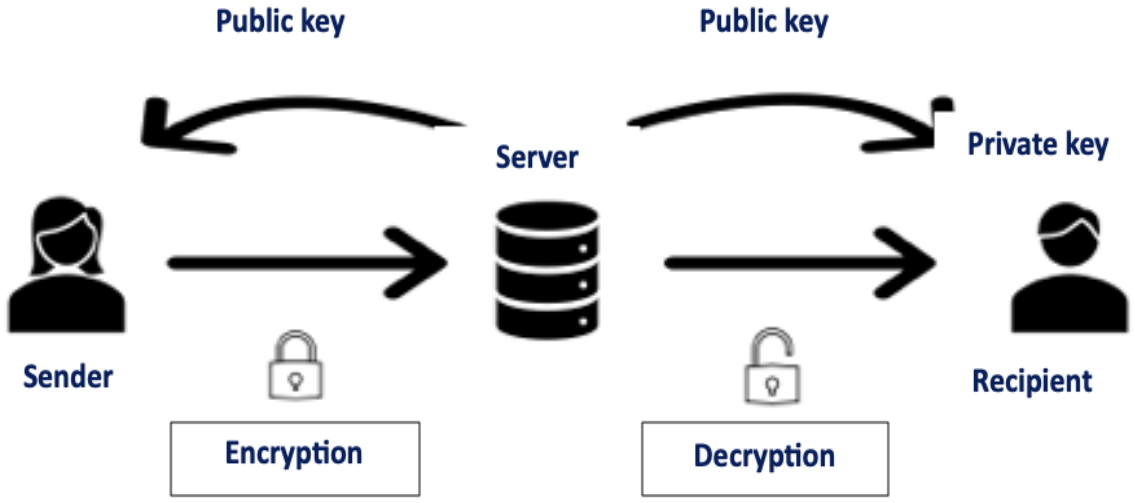

Figure 1: Example of end-to-end encryption

[1] S. O'DEA, "Number of smartphone users worldwide from 2016 to 2023", *Statista*, 31 March 2021. [Online] Available : [https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/]. (Accessed 14 June 2021).

End-to-end encryption (E2EE) is an encryption technique based on encryption and decryption using public and private keys, allowing communications to resist eavesdropping and surveillance attempts, including by service providers.

Many services, including **Signal**, **Pretty Good Privacy**, **WhatsApp**, and **Telegram** use end-to-end encryption. This method poses more problems for LEAs as the knowledge of the decryption keys is only known by the sender and the recipient of the communications, which essentially prevents any cooperation order that could be assigned to the encryption service providers.

There are several methods of encryption but the principle remains broadly the same. It is a technique that consists in making data secret by setting up an agreement between the parties. Encrypted messages can then only be decrypted by using a decryption key. The longer is the key, the more secure it remains. Symmetric encryption, which is typically used to encrypt hard drives, is a type of encryption in which a single key is used to encrypt and decrypt electronic information. Entities that would like to communicate using symmetric encryption must exchange this key in a secure manner so that it can be used in the decryption process. This method of encryption differs from asymmetric encryption where a pair of keys, one public and one private, is used to encrypt and decrypt messages, thus solving the problem of exchanging the secret key. This second method is therefore used to encrypt communications. Encryption makes it possible to guarantee the authenticity, integrity and confidentiality of the data transmitted since it ensures that the message has not been modified at the start and at the end. Thus, it guarantees a certain level of security in communications between individuals. In most cases, encryption is lawful, but sometimes this instrument for the security of individuals hinders the action of States in terms of fight against cybercrime by preventing the traceability of cybercriminals. Indeed, encryption is often used to commit offences because it allows the confidentiality of communications between criminals. Moreover, encryption is at the heart of the dark web and the deep web, as well as payments in crypto-currencies whose manipulation is conditioned by encryption. The means of communication are also encrypted in criminal matters by means of quite sophisticated means, as seen in the Encrochat[2] case (an encrypted telecommunications company). This case scenario is indicative of the many issues underlying encryption tools, which creates a conflict between citizens' Fundamental rights, such as their right to privacy and their right to a fair trial and the needs of law enforcement agencies for the proper conduct of their investigations.

In view of the potential hindrance of encryption in terms of security and crime-fighting, many stakeholders are in favour of weakening this tool. In a statement, the European Commission insisted that "we must ensure that the relevant law enforcement and judicial authorities are able to exercise their legal powers, both online and offline, to protect our societies and citizens"[3]. As an example of this gradual removal of access to encryption tools, the EU Council of Ministers adopted a draft resolution in November 2020 to ban encryption in the name of the fight against terrorism, entitled Security through encryption and despite encryption[4]. According to the Council, the obstacles posed by encryption outweigh the protection of fundamental rights and it would therefore be desirable to put in place "back doors" to facilitate access by intelligence services to encrypted communications. This highly liberticidal measure may seem surprising in view of the EU's reactions when countries less favourable to the guarantee of Fundamental rights put in place measures similar to this one.

---

[2] Forum international de la cybersécurité (FIC), "EncroChat: Deciphering of the End-to-End Encryption Service Used by Criminals - International Cybersecurity Observatory", *Observatoire du FIC*, 15 July 2020. [Online] Available: [https://observatoire-fic.com/en/encrochat-deciphering-of-the-end-to-end-encryption-service-used-by-criminals/]. (Accessed 14 June 2021).

[3] Council of the EU press release, "Encryption: Council adopts resolution on 'Security through encryption and despite encryption'", 14 December 2020. [Online] Available: [https://www.consilium.europa.eu/fr/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/].(Accessed on 14 June 2021).

[4] Council of the European Union, "Security through encryption and security despite encryption", 24 November 2020. [Online] Available [https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf].

Europe is always at the forefront to react in the name of Fundamental rights and does not fail to recall its resentment towards mass surveillance as demonstrated by the Court of Justice of the European Union (CJEU) in several of its decisions[5]. With this draft resolution, the EU is going against its original position in the name of the fight against terrorism, but at the same time is undermining the privacy of its citizens. What really prevails in this conflict between Fundamental rights? Disregarding encryption will certainly make it possible to detect offences in many cases, but it is difficult to anticipate the content of the decrypted data, that leads to compromising the privacy of the persons concerned. Moreover, it has been shown by encryption professionals[6] that this measure of limiting encryption would not necessarily be effective. These legal provisions apply to the general public, of which cybercriminals are rarely part. They know the ins and outs of the cyber domain and will be able to circumvent these constraints without concern, in particular by using products - which is already the case - that do not respect the legislation in force. This desire to weaken encryption is therefore considered in some aspects to be counterproductive. On the one hand, cybercriminals will continue to encrypt their communications by illegal means, and on the other hand, citizens will be all the more vulnerable because of facilitated decryption that will be made possible by these measures. Will the EU jeopardise the freedom and security of its citizens by banning the use of encryption tools, even though this has not been proven to be indisputably effective? Even if the use of encryption by cybercriminals is uncontested and therefore serves cybercrime, can't we consider that this tool is also a shelter for individuals and their rights in the digital age? For instance, the right to privacy of individuals is a Fundamental right that is protected and guaranteed at national as well as at European and international level. It is one of the fundamental principles of a democratic society. It can be found in many texts, such as the 1948 United Nations Universal Declaration of Human Rights[7]. It is a sacred and comprehensive right that includes several principals such as the protection of privacy and the secrecy of communications. Citizens have a range of legal and technical tools to protect this right that include encryption. The Council of Europe states the need for the implementation of encryption tools in order to insure the protection of privacy. Indeed, in the preamble to Chapter XI of its report entitled Final Report on the Seventh Round of Mutual Evaluations on the Practical Implementation and Functioning of European Policies for Preventing and Combating Computer-related Crime, it states : "The increasing availability and use of secure and reliable encryption technologies ensures the security, safe transmission and confidentiality of computer data and, consequently, the protection of the privacy of citizens and the effective protection of data in cyberspace"[8]. But what happens when, in the course of a criminal investigation, a seized phone is encrypted? How can the contents of this device be accessed legally and without compromising the Fundamental rights of its owner? The use of decryption methods in the context of zero-day policies or backdoors sometimes challenges the very essence of encryption. For example, some LEAs request that backdoors are created by software developers and devices manufacturers, allowing them a secret access into the software in order to observe or even control the activity taking place within the device. LEAs may find zero-day vulnerabilities, and develop zero-day exploits in order to compromise devices. In such case, if LEAs are not forcing anyone to disclose their passwords or forcing phone developers to place hidden backdoors, zero-day exploits could be considered by most

[5] CJEU, 6 October 2020, Case C-623/17, *Privacy International*, and in Joined Cases C-511/18, *La Quadrature du Net and Others*, C-512/18, *French Data Network and Others*, and C-520/18, *Ordre des barreaux francophones et germanophone and Others*. [Online] Available: [https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf].

[6] Observatoire des libertés et du Numérique, Positioning of the Observatoire des libertés et du Numérique on "Encryption, security and freedoms", *Ligue des droits de l'homme*, January 2017, p. 6. [Online] Available: [https://www.ldh-france.org/wp-content/uploads/2017/01/201701.OLN_.Chiffrementsecuritelibertes.pdf]. (Accessed on 16 June 2021).

[7] United Nations, *United Nations Universal Declaration of Human Rights*, 10 December 1948, art. 12. [Online] Available: [https://www.un.org/sites/un2.un.org/files/udhr.pdf].

[8] Council of the European Union, Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime", 2 October 2017 [Online] Available: [https://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/en/pdf].

jurisdictions and applicable laws as fairly 'legal'. Furthermore, criminal laws do not obligate anyone to reveal zero-day vulnerabilities as long as they don't compromise information systems with them. These zero-day vulnerability knowledge can also be considered as intangible asset of a company who develops smartphone forensic software. However, this may also become a controversial ethical issue, as they may reveal them with the aim of preserving consumer's security. These methods often violate the Fundamental rights of individuals since legitimate users of these devices are not aware that they can be monitored by law enforcement agencies. In the other hand, zero-day policies define what to do with zero-day vulnerabilities from software and hardware components.

In order to avoid the use of such methods that threaten fundamental rights as much as possible, it is necessary to put in place new tools to reconcile Fundamental rights and the proper conduct of investigations. This is the approach taken by the EXFILES project[9]. It is becoming increasingly difficult for LEAs to carry out their investigations because of encryption methods. Law enforcement agencies are trying to find new ways to access these encrypted contents. EXFILES aims to find software exploitation methods, hardware methods and combined methods to give law enforcement officers the tools and protocols to extract data quickly and consistently in strict legal contexts. New tools and methods, inspired by other areas of cyber security, are developed to lead to new forensic methods of accessing data for criminal investigations. This deliverable focuses mainly on the legal aspects of the research and exploitation of these new methods, and the legal and judicial background for cyberinvestigation.

It is necessary to pay attention to the legislative framework in which these new methods are developed in order to ensure their compliance with the various applicable law in the various countries contributing to the project and, in the longer term, in all the Member States of the European Union. LEAs' methods for decrypting or bypassing encryption are confronted with the expectations of citizens. The law is constantly seeking a balance between fundamental rights as freedom and security, and a solution must be found to respond to the need of LEAs to access encrypted content when necessary while respecting the fundamental rights of suspects and third parties. In order to minimise the infringement of citizens' rights and freedoms, this requires, among other things, information and transparency from LEAs and States about the used methods. But how far can this transparency go? It is difficult to require that LEAs' decryption methods are totally transparent, as this would compromise the very effectiveness of their work. Firstly, it would enable criminals to better circumvent the methods used by LEAs and to consolidate their techniques. Secondly, manufacturers would increase the security of their devices, necessarily undermining the effectiveness of progress made by LEAs.

Beyond this issue of transparency of the methods used by LEAs, one of the objectives of this deliverable is to put into perspective the existing judicial procedures in the different countries contributing to the project. This project is intended to benefit national and European law enforcement agencies by facilitating their search for and access to electronic evidences in cellphones and smartphones. Today, there is still no comprehensive and unified legal definition of electronic evidence, even though some countries define it in their legislation[10]. It is often equated with physical evidence, but in electronic format. Nevertheless, a distinction must be made between digital evidence and electronic evidence. Digital evidence is evidence that initially existed in analogue form and was subsequently dematerialised. Conversely, there is a consensus in the literature that electronic evidence is evidence that was originally digital (i.e. generated directly by electronic means or on the Internet). A distinction between natively digital data and digitised data would possibly serve to limit the cases in which a decryption procedure would have to be put in place. If law enforcement authorities know that a data is physically accessible, this would save time and avoid compromising Fundamental rights and freedoms by having to decrypt the data to obtain evidence of an offence.

[9] EXFILES, Europe fights against crime and terrorism project. [Online] Available: [https://exfiles.eu/about/]. (Accessed on 16 June 2021).

[10] European project on Evidence, "European Informatics Data Exchange Framework for Courts and Evidence", *Cordis* [https://cordis.europa.eu/project/id/608185].

As it does not have its own regime, electronic evidence is most of the time “housed” in the same category as physical evidence. It is governed by the law of evidence and the law of search and seizure, which is not entirely transposable to the digital domain, which can sometimes cause problems in the treatment of electronic evidence. One of the aims of this is to enable LEAs to have their evidence admissible in court. If evidence has been obtained unfairly or illegally, it will not be admissible in court under the presumption of innocence and the right to a fair trial, which are fundamental principles of criminal procedure[11]. This raises the problem of the adequacy of criminal procedure with the development of new technologies. The legislator is running behind technology and the rules applicable today are not always suitable to digital uses. When a cellphone is seized by the police, it is often encrypted. The decryption key is, in most cases, not communicated, which does not allow access to the contents of the device. The main characteristic of electronic evidence is its immateriality, it is not physical, it is not tangible and its integrity must be guaranteed to ensure its admissibility in court. There is a strict legal framework for the seizure of electronic material in which data that can be used as evidence is stored, but the legal framework is still incomplete and does not always allow for the implementation of a coherent policy of electronic evidence extraction without legal uncertainty. The collection of digital evidence must necessarily be subject to a rigorous procedure to ensure its integrity. Sometimes the data is encrypted and its clarification is then carried out by forensic experts.

Furthermore, if data is found in a mobile phone that is physically accessible from a national territory, this does not mean that the data is located in that same territory. The digital revolution, particularly through the Internet, has facilitated the removal of virtual borders. Cyberspace is a dematerialised territory that is not attached to any State, which makes its governance even more complex. Through cloud storage services, it is now possible to store data anywhere in the world, often without even knowing exactly where. With physical borders disappearing and the location of data being split across the world, it is often necessary for law enforcement to request the transfer of evidence from the authorities in the countries where the data is stored. This further hampers the work of law enforcement agencies in the fight against cybercrime because while electronic evidence is naturally characterised by its extraterritoriality, law enforcement agencies are hampered by the territoriality of its jurisdiction. Today, increasing cooperation between law enforcement agencies at an international level has become essential. Enhanced mutual legal assistance will make it possible to exchange electronic evidence without interfering in the sovereign domains of the other State and, at the same time, to fight cybercrime more effectively.

However, there are many problems with cross-border cooperation. First of all, the existing methods, both at the level of the Council of Europe and the European Union, are less and less effective. The Mutual Legal Assistance, aimed at facilitating judicial and police cooperation in obtaining evidence, particularly in the criminal field is decreasingly adapted to current challenges[12]. The procedures are long, tedious and raise the question of the very rationale of this type of cooperation tool. Moreover, criminal procedures, which are a matter of State sovereignty, differ greatly from one country to another. There is a great deal of heterogeneity in the rules governing the seizure of devices, methods of collecting evidence, the length of time devices and data kept, etc. This lack of legal harmonisation leads to a lack of clarity in the rules of procedure. This lack of homogeneity further hinders inter-state cooperation. Furthermore, as it is today, the international and European legislative frameworks failed to provide a unified regulation in this area and do not allow for effective harmonisation of existing rules.

However, national and international stakeholders are aware of the issues at stake and are currently addressing this matter into consideration. On Wednesday 14 April 2021, the Council of Europe's

[11] Council of Europe, *European Convention of Human Rights* (EConv.HR), 4 November 1950, art. 6 [Online] Available: [https://www.echr.coe.int/Documents/Convention_ENG.pdf].

[12] "Improving Cross-Border Access to Electronic Evidence", *System Upgrade*, January 2019 [Online] Available: [https://www.gppi.net/media/GPPi_2018_Hohmann_Barnett_System_Upgrade.pdf].

Committee of the Convention on Cybercrime (T-CY) published the first complete draft text of the second additional protocol to modernise the Budapest Convention on Cybercrime and invited interested parties to submit their comments by 2 May 2021. The Budapest Convention of 23 November 2001 is the first international treaty dealing with the problems of the Internet and the development of cybercrime that it induced. The Convention essentially aims to harmonise the elements of national substantive criminal law offences and related provisions on cybercrime, to provide national procedural criminal law with the necessary powers to investigate and prosecute such offences as well as other offences committed by means of a computer system or where evidence exists in electronic form, and to establish a swift and effective regime of international cooperation. However, the Council of Europe has not been able to anticipate all the developments in the digital field, which is why this text had to be reformed to meet current needs. The EU has also taken over this issue, in particular with the proposal of the E-Evidence package of 17 April 2017[13]. As a large majority of criminal investigations involve digital data, the European legislator wants to put in place a regulation for the benefit of law enforcement agencies to counteract new forms of cybercrime through effective means of obtaining electronic evidence. If successful, this will make it easier and faster for police and judicial authorities to obtain the electronic evidence they need to investigate and possibly prosecute criminals and terrorists.

Although there are many laws against cybercrime, the fact that cybercrime is carried out internationally raises problems regarding the territorial applicability of the law. Indeed, a foreign judgment is not enforceable in France and vice versa. As a consequence, difficulties remain in enforcing court decisions. Beyond that, there is the impression that the legislator is running behind the technological evolution and is often late in creating effective laws. The legal tool is not very effective and other means must be found to protect against cybercrime. However, one important thing to bear in mind is that these other devices will also have to be legally regulated.

In this context, when discussing the need to develop a legal response to the global challenge of cybercrime, especially due to deterritorialization, soft law has emerged as a key tool, as with attempts to regulate artificial intelligence. It has been argued that flexible law could be beneficial in dealing with technological developments. Thus, the concept of soft law, which originated in the field of international relations, has already been used on several occasions to facilitate international collaborations.

In cyberspace, a constantly changing environment, hard law has its own limitations, which can be complemented by soft law that is flexible, able to adapt to technological developments. For, in the international community, the absence of a central authority imposing obligations and sanctions shows that the characteristics of the internal hard law of States, do not present in the same way in in international society. As was expressed in the French Conseil d'État report that "obligations can only arise from the will of sovereign States"[14]. In other words, in this context, hard law poses its own limits when several states are involved; it is not possible to impose compliance with hard law on states in a binding manner, their obligations can only arise from their own will.

Faced with this difficulty of imposing obligations and sanctions, the interests of soft law come to the fore. However, flexible law instruments, such as flexible provisions in a treaty or non-conventional agreed acts, all have different functions and roles. In order to ensure an effectiveness that approaches hard law, it is possible to speak of a soft law, which is autonomous in regulating international relations and which will allow it to play a role, on a permanent basis, as a method of governance. This method is often used in the European Union to overcome institutional difficulties within its communities. The experience gained in developing non-binding solutions to problems of

[13] European Parliament and Council, "Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters", 17 April 2018 [Online] Available: [https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN].

[14] French Conseil d'État, Report on "Le droit souple", 2013 Annual study n° 64, 2013. [Online] Available: [https://www.vie-publique.fr/sites/default/files/rapport/pdf/144000280.pdf].

international law, which require cross-border cooperation, opens the way to solving problems of cybercrime.

However, the effectiveness of soft law is an important issue in this concept because, by its inherent in soft law is non-binding and thus it will be deemed to be effective provided its rules are followed.

In this first legal deliverable of the EXFILES project, we will, after a presentation of the main reference texts and supra-European stakeholders (Chapter 2), explore the law of the Union and of the partner countries through the prism of the fundamental rights (Chapter 3) that are challenged by the search for electronic evidence through decryption. We will then address the framework of investigations and evidence recovery and the many aspects it covers (Chapter 4). Finally, we will focus on one of the major issues that will have been the common thread linking fundamental rights to evidence preservation: the protection of the right to privacy through the protection of personal data (Chapter 5).

Chapter 2 Overview of the international legal framework and main stakeholders

In this first chapter, we will display an overview of the relevant international legal framework and soft law applicable or potentially applicable to the collection of digital evidence from mobile phones. Since the aim of digital forensics is to produce evidence at trials, electronic evidence must be obtained in compliance with existing legislation to ensure admissibility before courts.

The EXFILES project focuses mainly on criminal proceedings, we therefore focus the overall assessment on criminal law, even though regulation in other areas will be referred to where relevant. This legal framework includes but is not limited to cybercrime regulation, knowing “traditional” crimes also often include the use of mobile phones and cyberspace. Being a European project, EXFILES aims at exploring the European Union (EU) legal framework. In criminal proceedings however, even if international and European instruments of both hard and soft law outline cooperation and general principles on collection, preservation and exchange of electronic evidences, most of the regulation comes from national law of the Member States.

Criminal proceedings depend on evidence to establish the facts. Historically, evidence has always been either physical (e.g. with documents) or oral (e.g. with witness testimony). Electronic evidence is in some ways similar to this traditional type of evidence, in that it must present the same admissibility characteristic, have the same ability to demonstrate that it is unaltered and reflects the same information as at the time the offence was committed.

- It must be authentic, meaning that when it is produced before a court, it must establish the facts indisputably and be unquestionably similar to its original state.
- It must be complete so as not to leave room for the prism of interpretation.
- It must be reliable: it is here that the way in which it is collected and processed by forensics is of primary importance, for there must be no doubt as to its authenticity and veracity.
- It must be believable, i.e. able to convince of the facts it presents and the court must be able to rely on it as the truth.
- Finally, it must be proportional, meaning the method by which it was acquired must be proportionate to the interests of justice and must not prejudice the rights of the parties involved beyond its probative value.

In other ways however, this type of evidence is particular and has its own characteristics:

- It is often visible only to specialists, who search for it in locations that can only be reached by special forensic tools, which evolve very quickly and must be constantly renewed and updated
- It is particularly volatile, and can be altered by a simple power outage, and the electronic components can be degraded making it impossible to read the data. It even can be altered by normal use
- It has the unique advantage of being able to be copied without altering the original[15].

These peculiar features make of electronic evidences a challenge for justice systems, which requires specific methods to process these evidences while preserving their integrity and probative value, and ensuring they were not manipulated or altered. Electronic evidence has been qualified of “only

[15] Council of Europe, Directorate General of Human Rights and Rule of Law and Cybercrime Division, "Electronic Evidence Guide, a Basic Guide for Police Officers, Prosecutors and Judges", 2020, pp. 11-13 [Online] Available: [https://rm.coe.int/c-proc-electronic-evidence-guide-2-1-en-june-2020-web3/16809efd7f].

as valuable as the integrity of the method the evidence was obtained”16, and the digital forensic investigation is subject to considerable scrutiny of both the integrity of the evidence and the integrity or reliability of the investigation process. The reliability of the digital investigation process can only be demonstrated consistent to the relevant regulatory framework through all the collection, conservation, communication and presentation steps.

As collection of electronic evidence and forensic methods may usually mean an infringement of a person’s fundamental rights to private life and protection of personal data17, “the design, manufacture and use of detection technologies and associated technologies, together with legislation or other measures aiming to regulate or promote them, must fully comply with Fundamental Rights as provided for in the EU Charter of Fundamental Rights and the European Convention on Human Rights. Particular attention must be paid to compliance with the protection of personal data and the right to private life”18. Tracking or searching a smartphone implicate both the right to privacy and to communication secrecy of a person, therefore forensic methods and technologies must ensure compliance with the relevant legal framework.

The rules regarding criminal proceedings have little focus on evidence and vary considerably from State to State, “even amongst countries with similar legal traditions”19, as stated by the United Nations Office on Drugs and Crime in its 2013 Comprehensive Study on Cybercrime. Moreover, some states apply traditional laws on electronic evidence, others adapted their legislation regarding evidence to integrate specific rules for digital forensics investigation. Although the situation has evolved considerably since 2013, there is still no overall international legal framework regarding electronic evidence. However, international conventions apply to this field, reinforced and clarified by guidelines and technical standards, and cooperation mechanisms have been developed, in particular by the Council of Europe.

In this chapter, we set the scene by examining the international legal framework regarding fundamental rights, processing of electronic evidence, and international cooperation, provided by the main stakeholders at the international scale relevant to EU countries, which we are going to identify. The European Union and national partner States legal framework will be further discussed in the following chapters.

2.1 The United Nations provisions

The international organisation was founded in 1945 and counts 193 members since 2011. All 27 EU Member States are represented at the United Nations (UN) General Assembly, where the EU itself

[16] David W. Bennett, "The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations", *Forensic Focus*, 22 August 2011 [Online] Available: [https://www.forensicfocus.com/articles/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/].

[17] Commission of the European Communities, Green paper on "Detection Technologies in the Work of Law Enforcement, Customs and Other Security Authorities", 1 September 2006, p. 5 [Online] Available: [https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0474:FIN:EN:PDF].

[18] European Commission, "Memo on the Green Paper on Detection and Associated Technologies in the Work of Law Enforcement, Customs and Other Security Authorities", 4 September 2006, p. 3 [Online] Available: [https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_06_317/MEMO_06_317_EN.pdf]
.

[19] United Nations Office on Drugs and Crime (UNODC), "Comprehensive Study on Cybercrime", *United Nations Office on Drugs and Crime*, February 2013, p. 158 [Online] Available: [https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf].

has an Observer status. One Member State, France, sits as a permanent member at the Security Council.

UN principles and mission of work are guided by the Charter of the United Nations [20]. Three of the main objectives described are relevant to our work:

- Protecting human rights, through the promotion of the Universal Declaration of Human Rights
- Maintain international peace and security, especially through its counter-terrorism mission
- Support international law, establishing the conditions under which justice and compliance with obligations under treaties and other sources of international law can be maintained

The Universal Declaration of Human Rights, adopted in 1948 by the UN General Assembly, enshrines the rights and freedoms of individuals. While not a treaty itself, the Declaration was explicitly adopted for the purpose of defining the meaning of "fundamental freedoms" and "human rights" appearing in the United Nations Charter, and has served as the foundation for the International Covenant on Civil and Political Rights, and other Human Rights binding conventions, at the European level for instance.

At the international level, it is the United Nation Office on Drugs and Crime that gives us a first definition of electronic evidence in its *Comprehensive Study on Cybercrime*:

> **"*Evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established.***
>
> ***Electronic evidence is all such material that exists in electronic, or digital, form*"[21].**

This type of evidence is increasingly important in all forms of crime, not only cybercrime. Some common principles are recalled: the gathering and processing of electronic evidence must guarantee the integrity, authenticity and continuity of the evidence throughout the chain of custody, from its seizure to its use in a court of law.

Through the following paragraphs, we will examine how the UN addresses some basic principles related to fundamental rights, justice, international cooperation and the processing of electronic evidence.

2.1.1 United Nations' International Covenant on Civil and Political Rights

Entered into force in March 1976, the International Covenant on Civil and Political Rights has been ratified by 173 countries, and signed by 6 more. This covenant does not address cross-border cooperation in criminal matters or gathering of evidence, but it reaffirms human rights that should be guaranteed by the States, relevant in prosecution as they relate to the balance between fundamental rights and security:

Article 2 (3) "*Each State Party to the present Covenant undertakes:*

[…] (b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy";

[20] United Nations (UN), *Charter of the United Nations*, 26 June 1945 [Online] Available: [https://www.un.org/en/about-us/un-charter/full-text].

[21] UNODC, "Comprehensive Study on Cybercrime", *op. cit.*, p. 157.

Article 9 (1) "*Everyone has the right to liberty and security of person. No one shall be subjected to arbitrary arrest or detention. No one shall be deprived of his liberty except on such grounds and in accordance with such procedure as are established by law*."

Article 14 (1) "*All persons shall be equal before the courts and tribunals. In the determination of any criminal charge against him, or of his rights and obligations in a suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law*".[22]

It settles that States need competent law enforcement and judicial systems, and laws in order to prosecute (cyber)crimes, without which felonies could not even exist.

The Article 17 addresses the right to privacy:

"(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

(2) Everyone has the right to the protection of the law against such interference or attacks."

Privacy and communications should therefore be protected by the law

2.1.2 United Nation's Convention against Transnational Organise Crime

The United Nations Convention against Transnational Organised Crime, entered into force in September 2003, has 190 parties, including the European Union[23].

Its purpose, stated in Article 1, is to "*promote cooperation to prevent and combat transnational organized crime more effectively"*[24].

It applies to the prevention, investigation and prosecution of participation in an organized criminal group (as defined in Article 5), laundering of proceeds of crime (as defined in Article 6), corruption (Article 8), obstruction of justice (Article 23), and serious crimes, defined in the Article 2 (a) as "*conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty*".

[22] United Nations Office of the High Commissioner on Human Rights (OHCHR), *International Covenant on Civil and Political Rights*, 16 December 1966 [Online] Available: [https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx].

[23] United Nations, *United Nations Convention against Transnational Organized Crime*, New York, 15 November 2000 [Online] Available: [https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=_en]. [accessed 29 July 2020].

[24] UNODC, *United Nations Convention Against Transnational Organized Crime and the Protocols Thereto*, New-York, 2004, p. 6 [Online] Available: [https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf].

The Convention defines the transnational nature of an offence in its article 3, paragraph 2, thus indicating several scenarios in which States Parties are entitled to request cooperation from other States:

"[…] *an offence is transnational in nature if:*

(a)It is committed in more than one State;

(b)It is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State;

(c)It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or

(d)It is committed in one State but has substantial effects in another State."[25]

While international cooperation is drawn by the Convention, sovereignty of States Parties is reasserted in Article 4 with the principle of "non-intervention in the domestic affairs of other States"[26]. Evidence is approached in the Article 12 as follows:

"*Article 12. Confiscation and Seizure:*

1. States Parties shall adopt, to the greatest extent possible within their domestic legal systems, such measures as may be necessary to enable confiscation of:

(a)Proceeds of crime derived from offences covered by this Convention or property the value of which corresponds to that of such proceeds;

(b)Property, equipment or other instrumentalities used in or destined for use in offences covered by this Convention.

2. States Parties shall adopt such measures as may be necessary to enable the identification, tracing, freezing or seizure of any item referred to in paragraph 1 of this article for the purpose of eventual confiscation.

3. If proceeds of crime have been transformed or converted, in part or in full, into other property, such property shall be liable to the measures referred to in this article instead of the proceeds.

4. If proceeds of crime have been intermingled with property acquired from legitimate sources, such property shall, without prejudice to any powers relating to freezing or seizure, be liable to confiscation up to the assessed value of the intermingled proceeds.

[…]"[27]

These dispositions can readily be applied to electronic evidence, even if this particular type of evidence is not explicitly mentioned. Cooperation for purposes of confiscation is addressed in the next article, inviting States Parties to the Convention to submit a request to the competent authority of the country concerned to obtain an order of confiscation and to be entitled to execute it, and to submit a confiscation order issued by a Court in the territory of the requesting State Party. The requested State Party "*shall take measures to identify, trace and freeze or seize proceeds of crime, property, equipment or other instrumentalities referred to in article 12, paragraph 1, of this Convention for the purpose of eventual confiscation to be ordered either by the requesting State Party or* […] *by the requested State Party*"[28].

The main limitation to this international cooperation instruments remains the differences between domestic legislation of the requested and the requesting States. States Parties are encouraged to

[25] *Idem.*

[26] *Idem,* p. 7.

[27] *Idem,* p. 12.

[28] *Idem,* p. 13.

conduct bilateral or multilateral agreements for joint investigations in Article 19, and to mutual legal assistance in Article 18 (3) for several purposes, including:

"(a) Taking evidence or statements from persons;

[…]

(c) Executing searches and seizures, and freezing;

(d) Examining objects and sites;

(e) Providing information, evidentiary items and expert evaluations;

(f) Providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records;

(g) Identifying or tracing proceeds of crime, property, instrumentalities or other things for evidentiary purposes;

[…]"[29]

The process towards international cooperation in the collection and exchange of evidence for criminal prosecutions was already under way in 2000, although at that time much remained to be done both to define and prosecute cybercrime – which was not even mentioned in this Convention – and to adjust the different national legal frameworks to improve cooperation in the prosecution of crimes.

2.1.3 Interpol

The International Criminal Police Organization, known as INTERPOL, is the world's largest police organization, with 194 member states, each one represented in the General Assembly. Created in 1923 as the International Criminal Police Commission, it officially became INTERPOL with its 1956 Constitution [30]. Its main purpose is to bond law enforcement agencies of the member states, as it is not a law enforcement agency itself.

INTERPOL is not an arm of the United Nations, but the two organizations decided to join forces in 1996, and INTERPOL became a Permanent Observer at the United Nations[31]. They cooperate primarily in the fields of counter-terrorism, organized crime and emerging crime, human trafficking and migrant smuggling, and on the ground with united nations entities such as the United Nations Office on Drugs and Crime [32].

The Article 2 of the Constitution of International Criminal Police Organization defines INTERPOL's aim as follows:

"(1) To ensure an promote the widest possible mutual assistance between all criminal police authorities within the limits of the laws exist in in the different countries and in the spirit of the "Universal Declaration of Human Rights";

[29] *Idem*, p. 20.

[30] INTERPOL Office of legal affairs, *Constitution of the International Criminal Police Organization*, 1956 [Online] Available: [https://www.interpol.int/content/download/590/file/Constitution%20of%20the%20ICPO-INTERPOL-EN.pdf].

[31] INTERPOL, "INTERPOL and the United Nations", [Online] Available: [https://www.interpol.int/en/Our-partners/International-organization-partners/INTERPOL-and-the-United-Nations]. [Accessed 12 August 2020].

[32] INTERPOL, "Today's Priorities for UN-INTERPOL Collaboration", [Online] Available: [https://www.interpol.int/en/Our-partners/International-organization-partners/INTERPOL-and-the-United-Nations/Today-s-priorities-for-INTERPOL-United-Nations-collaboration]. [Accessed 12 August 2020].

(2) To establish and develop all institutions likely to contribute effectively to the prevention and suppression of ordinary law crimes." [33]

To achieve its mission, contributing to the prevention and suppression of crimes, the core activity of the organization is the exchange of information and the construction of large databases on crimes and fight against crime. For this reason, in 1974 the General Assembly formalized the importance of privacy in INTERPOL's operations and later created an independent data protection authority [34, 35].

One of INTERPOL's fields of intervention is cybercrime. The borderless nature of cybercrime and the increase in cyber-enabled crime make more essential than ever for law enforcement agencies to cooperate and exchange information at an international level and at a fast pace. INTERPOL contributes to coordinate a global response to cyberthreats with its "*Global cybercrime strategy"* [36] by, inter alia, providing access to and exploitation of raw digital data, promoting the exchange and analysis of information, enhancing interoperability, harmonization, providing electronic evidence management process, cyber training and expert investigative support, and participating in the development of digital forensic methods.

Although it is the largest in terms of membership, the United Nations is not the only organization playing a key role regarding law enforcement on the international stage.

2.2 The founding contributions of the Council of Europe

The Council of Europe was established by the Treaty of London on 5 May 1949, it is not an institution of the European Union. Members of the Council of Europe include all European Union Member States, but is not limited to them[37]. Forty-seven countries are Member States, representing the European continent and Russia, and six more are Observer States, a status dedicated to non-European democracies embracing "*the values of the Council of Europe, which are pluralist democracy, the rule of law and respect for human rights and fundamental freedoms*" [38].

The Council of Europe provided several instruments regarding combating cybercrime, cyber-enabled crime, and relevant to electronic evidence; including the first binding treaty as a basis for international cooperation in this field.

2.2.1.1 Definition of electronic evidence

In its "Electronic evidence Guide", the Council of Europe defines electronic evidence as "*Any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings*" and specifies that "*electronic evidence is derived from*

[33] INTERPOL Office of legal affairs, *Constitution of the International Criminal Police Organization*, *op. cit.*, p. 3.

[34] INTERPOL, "Data Protection", [Online] Available: [https://www.interpol.int/en/Who-we-are/Legal-framework/Data-protection]. [Accessed 12 August 2020].

[35] INTERPOL, "Commission for the Control of INTERPOL's Files (CCF)", [Online] Available: [https://www.interpol.int/en/Who-we-are/Commission-for-the-Control-of-INTERPOL-s-Files-CCF]. [Accessed 29 August 2020].

[36] INTERPOL, *Global Cybercrime Strategy - Summary*, 2016 [Online] Available: [https://www.interpol.int/en/content/download/5586/file/Summary_CYBER_Strategy_2017_01_EN%20LR.pdf].

.

[37] Council of Europe, "Our Member States", [Online] Available: [https://www.coe.int/en/web/about-us/our-member-states]. [Accessed 20 August 2020].

[38] Council of Europe, Committee on Political Affairs and Democracy of the Parliament Assembly, *Establishment of a "Partner for Democracy" Status with the Parliamentary Assembly*, 14 May 2009 [Online] Available: [http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=12191&lang=en].

electronic devices such as computers and their peripheral apparatus, computer networks, mobile telephones, digital cameras and other portable equipment (including data storage devices), as well as from the Internet. The information it contains does not possess an independent physical form.

However, in many ways, electronic evidence is no different from traditional evidence in that the party introducing it into legal proceedings must be able to demonstrate that it reflects the same set of circumstances and factual information as it did at the time of the offence. In other words, they must be able to show that no changes, deletions, additions or other alterations have (or might have) taken place."[39]

Like any other evidence, electronic evidence must be authentic, complete, reliable, believable and gathered with proportional means to be used in court.

2.2.2 European Convention on Human Rights and Fundamental Freedoms

The European Convention on Human Rights and Fundamental Freedoms (ECONV.HR) came into force in 1953, and was the first instrument to give effect to certain of the rights stated in the Universal declaration of Human Rights. It has been amended and supplemented by numerous Protocols since then, and ratified by forty-seven Member States and the European Union[40].

The ECONV.HR enshrined the rights to freedom and security in its article 5, to a fair trial in Article 6, and to respect for private and family life in Article 8 [41].

However, this right to privacy of life, home and correspondence has some limitations:

"(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The collection of data as electronic evidence is permitted by this article 8 (2). However, the Council of Europe's values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights should govern all that occurs in cyberspace as well as they do outside cyberspace, to ensure it remains an area of freedoms and rights. The most difficult balance to find regarding these fundamental rights is between security on the one hand and freedom and privacy on the other. Therefore, the rules for processing of such data by the competent public authorities must take into account some privacy safeguards.

2.2.3 The Convention on Cybercrime

The Committee of Experts on Crime in Cyberspace (PC-CY) of the Council of Europe was created in 1996 in order to work on cybercrime issues, facing its fast-paced development. The final draft of the Convention on Cybercrime was approved by the European Committee on Crime Problems (CDPC) in June 2001 and submitted to the Committee of Ministers for adoption and opening for

[39] Directorate General of Human Rights and Rule of Law and Cybercrime Division, "Electronic Evidence Guide, a Basic Guide for Police Officers, Prosecutors and Judges", *op. cit.*

[40] Council of Europe, *European Convention on Human Rights and Fundamental Freedoms* (EConv.HR), *op. cit*.

[41] *Idem*, p. 8 – 11.

signature. It has been opened for signature in Budapest on 23 November 2001 [42], which earned it the name of "Budapest Convention".

A total of 65 countries are Parties to the Convention, 11 more are signatories or are invited to accede. All EU Member States are Parties to the Convention, except Sweden and Ireland, which have signed but not ratified the Convention and have an Observer status at the Budapest Convention [43]. Some non-European countries are Member States of the Convention, as Canada, Japan, or United States of America.

The Budapest Convention entered into force in 2004 and was the first – and remains the most relevant – international treaty on cybercrime and electronic evidence. It serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between State Parties to this treaty[44]. It provides for:

- The criminalization of conduct ranging from illegal access, data and systems interference to computer-related fraud and child pornography;
- Procedural law tools to investigate cybercrime and secure electronic evidence in relation to any crime;
- The harmonization of domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime;
- Set up a fast and effective regime of international cooperation[45].

[42] Council of Europe, *Explanatory Report to the Convention on Cybercrime*, 23 November 2001, p. 1 [Online] Available: [https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561].

[43] Council of Europe - Cybercrime, "Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY", [Online] Available: [https://www.coe.int/en/web/cybercrime/parties-observers]. [Accessed 2 August 2020].

[44] European Union Agency for Cybersecurity (ENISA), "Cooperation between CSIRTs and Law Enforcement: Interaction with the Judiciary", *ENISA*, November 2018 [Online] Available: [https://www.enisa.europa.eu/publications/csirts-le-cooperation]. [Accessed 5 May 2020].

[45] Council of Europe, *Explanatory Report to the Convention on Cybercrime*, *op. cit.*, p. 4.

Substantive criminal law: offences	Procedural law to secure evidence and investigate	International cooperation
Art. 2 – Illegal access	Art. 14 – Scope of procedural provisions	Art. 23 – General principles
Art. 3 – Illegal interception	Art. 15 – Conditions and safeguards	Art. 24 – Extradition
Art. 4 – Data interference	Art. 16 – Expedited preservation	Art. 25 – General rules
Art. 5 – System interference	Art. 17 – Expedited preservation and partial disclosure of traffic data	Art. 26 – Spontaneous information
Art. 6 – Misuse of devices	Art. 18 – Production order	Art. 27 – MLA in absence of treaty
Art. 7 – Computer-related forgery	Art. 19 – Search and seizure	Art. 28 – Confidentiality
Art. 8 – Computer-related fraud	Art. 20 – Real-time collection traffic data	Art. 29 – Expedited preservation
Art. 9 – Child pornography	Art. 21 – Interception of content data	Art. 30 – Partial disclosure traffic data
Art. 10 – IPR offences		Art. 31 – MLA accessing data
Art. 11 – Attempt, aiding, abetting		Art. 32 – Transborder access
Art. 12 – Corporate liability		Art. 33 – MLA collection traffic data
		Art. 34 – MLA interception content
		Art. 35 – 24/7 point of contact

Figure 2: Areas covered by the Budapest Convention[46].

Articles 2 to 12 of the Budapest Convention list offences against and by means of computers which must be covered by domestic laws of the Member States. The described offences must be criminalized and the criminal justice authorities of the Member State must be entitled by their procedural law to investigate cybercrime and any offence where evidence is in electronic form. A legislation consistent with the Convention facilitates international cooperation, as some of the domestic procedural powers addressed from Article 14 to Article 21 have a corresponding provision in international cooperation instrument, displayed from Article 23 to 35 [47] (see Table 1).

Adjusting national legal frameworks should then be a priority for Member States to enhance international cooperation, as well as updating and developing cybersecurity strategies and a regulatory framework regarding cyberspace.

The Convention specifically addresses cybercrime, but as noted by the European Data Protection Supervisor (EDPS) [48], electronic evidence may not necessarily flow from cybercrime but may also be processed in proceedings of traditional crimes, therefore, electronic evidence may be collected, preserved, used and exchanged in the same manner in criminal investigations of both cybercrimes and traditional crimes. The Budapest Convention's provisions, although applying primarily to cybercrime, should therefore apply to any electronic evidence.

The Convention contains several provisions on collecting electronic evidence in its "*Section II – Procedural Law*":

- Article 14 provides that the States Parties to the Convention shall adopt legislation and measures in order to establish powers and procedures for criminal investigations and proceedings to be applied to the offences referred to in the Convention, other criminal

[46] Council of Europe, Cybercrime Convention Committee, "The Budapest Convention on Cybercrime: Benefits and Impacts in Practice", 13 July 2020, p. 5 [Online] Available: [https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac].

[47] *Ibid.*

[48] European Data Protection Supervisor (EDPS), "EDPS Opinion on Proposals Regarding European Production and Preservation Orders for Electronic Evidence in Criminal Matters", 2019 [Online] Available: [https://edps.europa.eu/sites/edp/files/publication/19-11-06_opinion_on_e_evidence_proposals_fr.pdf].

offences committed by means of a computer system, and the collection of electronic evidence;
- Article 16 and Article 17 empower the States Parties national competent authorities for expedited preservation of stored computer data and expedited preservation and partial disclosure of traffic data;
- Article 18 empowers the Party's competent authority to order persons to submit specified computer data, and service providers to submit subscriber information;
- Article 19 empowers the Party's competent authority to search and seize of stored computer data;
- Article 20 empowers the authority to collect real-time traffic data; and
- Article 21 empowers the competent authority to intercept content data by collecting or recording, and to compel a service provider to co-operate or collect content data for the competent authority. [49]

These articles outline procedural measures to collect electronic evidence, while allowing national authorities to achieve the objectives through other measures should their domestic legal principles require so.

Some safeguards are given in Article 15:

"*(1) Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.*

(2) Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

(3) To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties."[50]

Law enforcement should execute investigative powers and procedures with regard for human rights and freedoms under European Convention on Human Rights (EConv.HR) and the United Nations International Covenant on Civil and Political Rights (ICCPR) discussed in the previous parts of this report, and with regard for the principle of proportionality.

On this last notion, the EDPS offers a handy toolkit to assess the proportionality of measures that limit the right to protection of personal data [51], in which it relies notably on the case law of the European Court of Human Rights and the Court of Justice of the European Union to provide support for the interpretation of this notion of proportionality.

The general safeguards enshrined by the Article 15 are not specific to the risks associated with the particular measures covered by the Convention, and the article does not enforce the establishment of the cited independent authority to supervise law enforcement actions empowered by the Convention, which nevertheless authorizes overriding fundamental rights. Nor does it provide for harmonization between State Parties for the respect of these fundamental rights in domestic legal

[49] Council of Europe, *Convention on Cybercrime, op. cit.*

[50] *Idem*, p. 8.

[51] EDPS, "Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit", 2017 [Online] Available: [https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_fr.pdf].

frameworks, even though some of the States Parties that are members of the Convention are not members of the EU or the Council of Europe, where their protection rules may not apply.

The jurisdiction issue is addressed in Article 22 of the Convention. States Parties to the Convention are required to adopt legislative and other measures necessary to establish jurisdiction over the offences mentioned in the Cybercrime Convention when the offence is committed in its territory, on board a ship flying the flag of that Party, on board an aircraft registered under the laws of that Party or when the offence is committed by one of the nationals of a States Party, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State [52]. The choice of jurisdiction is grounded in the principles of territoriality and nationality, and where more than one Party is involved, they are encouraged in Article 22 (5) to "*consult with a view to determining the most appropriate jurisdiction for prosecution*" [53].

However, two scenarios have to be distinguished when dealing with the question of jurisdiction in the case where electronic evidence is not physically located within the jurisdiction:

- Where an investigator has taken control of a computer that is connected to the Internet. In such circumstances, the investigator may have the power to click on websites or enter computers in other jurisdictions. The authority to do so may be given to the investigator by virtue of domestic law or a combination of domestic law and the provisions of Article 32 of the Budapest Convention on Cybercrime. (However, the country where the actual servers or computers are physically located may take another view)
- Where electronic evidence is located in the 'cloud' – that is, where the e-mails of a suspect, for instance, are not stored in their home computer, but are stored elsewhere on a separate hard drive in a foreign jurisdiction.

In each of these two sets of circumstances, investigating authorities will have to take different actions depending on the laws that apply[54].

To address the 'Cloud' challenge, negotiations on a second Additional Protocol to the Convention on Cybercrime on enhanced international cooperation and access to evidence in the cloud have been carried on[55], leading to the adoption of this protocol by the Committee of Ministers on November 2021.

On the approved text, the Cybercrime Convention Committee addresses the use of video conferencing for testimony and statements to be taken from a witness or expert, the introduction of joint investigations and joint investigation teams, the implementation of an emergency mutual assistance mechanism, the empower each Party's competent authority to order direct disclosure of subscriber information to a service provider (to resolve the above mentioned cloud challenge), and a provision to empower each Party's competent authority to give effect to order from another Party for expedited production of data. [56]

[52] Council of Europe, *Convention on Cybercrime*, *op. cit.*, p. 11.

[53] *Idem*, p. 12.

[54] Directorate General of Human Rights and Rule of Law and Cybercrime Division, "Electronic Evidence Guide, a Basic Guide for Police Officers, Prosecutors and Judges", *op. cit.*, p. 156.

[55] Council of Europe, Cybercrime Convention Committee, *Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime*, 23 June 2019 [Online] Available: [https://rm.coe.int/t-cy-2019-19-protocol-tor-extension-chair-note-v3/16809577ff].

[56] Council of Europe, Cybercrime Convention Committee, *Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime. Provisional Text*, 2020 [Online] Available: [https://rm.coe.int/t-cy-2018-23rev-protoprov-pub-text-v8a/16809f0cee] ; and Council of Europe, "Explanatory report to the Second Additional Protocol as noted by

The EDPS already commented the draft of the Second Additional Protocol and suggested that it should contain *"a clause providing that Member States shall, in their mutual relations, continue to apply rules of the European Union rather than the Second Additional Protocol"* to protect privacy with efficiency [57].

Chapter three of the Convention addresses international cooperation. The Article 23 on general principles relating to international cooperation provides that "*the States Parties shall cooperate with each other, in accordance with the principles of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence*".

The mentioned principles are developed in Articles 24 to 35 and relate to extradition, mutual assistance, spontaneous information, procedures pertaining to mutual assistance requests in the absence of applicable international agreements, confidentiality and limitation on use, expedited disclosure of preserved traffic data, mutual assistance regarding accessing of stored computer data, trans-border access to stored computer data with consent or where publicly available, mutual assistance regarding the real-time collection of traffic data and the interception of content data, and a 24/7 network.

2.2.4 The Convention on Mutual Assistance in Criminal Matters, and its additional protocols

The Convention on Mutual Assistance in Criminal Matters, entered into force on 12 June 1962, has 50 States Party which includes all Member States of the EU.

Its scope does not cover electronic evidence but, with its two Additional Protocols from 1978 [58] and 2001[59], it is the most far-reaching mutual assistance initiative, with details on the exchange of evidence, the hearing of witnesses, experts and prosecuted persons in cross-border criminal cases.

Evidence is handled in the Convention in Chapter II – Letters rogatory:

"*Article 3*

(1) The requested Party shall execute in the manner provided for by its law any letters rogatory relating to a criminal matter and addressed to it by the judicial authorities of the requesting Party for the purpose of procuring evidence or transmitting articles to be produced in evidence, records or documents.

[…]

---

the Committee of Ministers on 17 November 2021", 17 November 2021 [Online] Available: [https://rm.coe.int/1680a49c9d].

[57] EDPS, "EDPS Opinion on Proposals Regarding European Production and Preservation Orders for Electronic Evidence in Criminal Matters", *op. cit.*, p. 18.

[58] Council of Europe, *Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, 17 March 1978 [Online] Available: [https://rm.coe.int/1680077975].

[59] Council of Europe, *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, 8 November 2001 [Online] Available: [https://www.coe.int/en/web/conventions/-/council-of-europe-second-additional-protocol-to-the-european-convention-on-mutual-assistance-in-criminal-matters-ets-no-182-translations].

(3) The requested Party may transmit certified copies or certified photostat copies of records or documents requested, unless the requesting Party expressly requests the transmission of originals, in which case the requested Party shall make every effort to comply with the request." [60]

The Article 24 of the Second Additional Protocol adds:

"*At the request of the requesting Party, the requested Party, in accordance with its national law, may take provisional measures for the purpose of preserving evidence, maintaining an existing situation or protecting endangered legal interests*." [61]

The main problem addressed in this Convention with respect to evidence is the exchange, not the collection of evidence, the aim being to create opportunities for competent authorities to approach each other. Nevertheless, the above articles apply most appropriately to electronic evidence.

Issues on privacy and data protection were not addressed in the 1959 Convention, but are in the 2001 Second Additional Protocol as follows:

"*Article 26 – Data protection*

(1) Personal data transferred from one Party to another as a result of the execution of a request made under the Convention or any of its Protocols, may be used by the Party to which such data have been transferred, only:

(a) for the purpose of proceedings to which the Convention or any of its Protocols apply;

(b) for other judicial and administrative proceedings directly related to the proceedings mentioned under (a);

(c) for preventing an immediate and serious threat to public security.

(2) Such data may however be used for any other purpose if prior consent to that effect is given by either the Party from which the data had been transferred, or the data subject.

(3) Any Party may refuse to transfer personal data obtained as a result of the execution of a request made under the Convention or any of its Protocols where:

– such data is protected under its national legislation, and

– the Party to which the data should be transferred is not bound by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, done at Strasbourg on 28 January 1981, unless the latter Party undertakes to afford such protection to the data as is required by the former Party.

(4) Any Party that transfers personal data obtained as a result of the execution of a request made under the Convention or any of its Protocols may require the Party to which the data have been transferred to give information on the use made with such data.

(5) Any Party may, by a declaration addressed to the Secretary General of the Council of Europe, require that, within the framework of procedures for which it could have refused or limited the transmission or the use of personal data in accordance with the provisions of the Convention or one of its Protocols, personal data transmitted to another Party not be used by the latter for the purposes of paragraph 1 unless with its previous consent." [62]

---

[60] Council of Europe, *European Convention on Mutual Assistance in Criminal Matters*, 20 April 1959 [Online] Available: [https://rm.coe.int/16800656ce].

[61] Council of Europe, *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, *op. cit.*, p. 13.

[62] Council of Europe, *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, *op. cit.*, p. 14.

Common principles of data protection and exemptions are present in this article, including consent and information on the intended purpose of the processing of transferred data. Reference is made to the 1981 *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* [63], which has since been modernised to cope with technological developments and became in 2018 the Convention 108+.

2.2.4.1 The Convention 108+

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS N°108) has been for forty years the only international legally binding instrument on the protection of private life and personal data open to any country in the world, and has 55 States Parties. The 18 May 2018, a Protocol (CETS N°223), amending the Convention was adopted by the Council of Europe's Committee of Ministers [64].

The Protocol has been signed by 35 Council of Europe Member States, as well as Argentina, Uruguay and Tunisia. As of now, 5 countries ratified it: Serbia, Poland, Lithuania Croatia and Bulgaria. The entry into force of the Protocol is conditional either on its ratification by all Parties to the Convention, or on its ratification by at least 35 Parties, in the latter case it will enter into force on 11 October 2023.

The amended Convention 108+ defines some terms related to the processing of personal data, in order to harmonize subsequent domestic law. It can be noted that the definition of personal data is broad and includes data that allows the direct or indirect identification or individualisation of a person, regardless of the knowledge of his or her civil or legal identity [65]. The Convention 108+ applies to all data processed in a Member States jurisdiction, regardless of the controller is in the public or private sector, the exception being data processing carried out by an individual in the course of purely personal or household activities (Article 3). It therefore applies to personal data in electronic evidence, processed by law enforcement and the judiciary. The Convention addresses in its Chapter II "*basic principles for the protection of personal data*": legitimacy of data processing, special categories of data, data security, transparency of processing, rights of the data subject. In the Article 11, some limitations and exceptions to these principles are exposed, notably for the purpose of "*national security, defence, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest*" [66].

Chapter III, particularly the Article 14, focuses on transborder flow of personal data. As stated in the explanatory document, "*the purpose of the transborder flow regime is to ensure that personal data originally processed within the jurisdiction of a Party (data collected or stored there, for instance), which is subsequently under the jurisdiction of a State which is not Party to the Convention continues to be processed with appropriate safeguards*"[50]. Although the convention does not build a single legal framework in all State Parties, it is specified that while there may be a wide variety of systems

[63] Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 28 January 1981 [Online] Available: [https://rm.coe.int/1680078b37].

[64] Council of Europe - Data Protection, "Convention 108+ : The Modernised Version of a Landmark Instrument", 18 May 2018 [Online] Available: [https://www.coe.int/en/web/data-protection/newsroom/-/asset_publisher/7oll6Oj8pbV8/content/modernisation-of-convention-108]. [Accessed 5 May 2020]

[65] Council of Europe, *Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 10 October 2018 [Online] Available: [https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a].

[66] Council of Europe, *Convention 108+ Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, June 2018, p. 9 [Online] Available: [https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1].

of protection, protection afforded has to be of such quality as to ensure that human rights are not affected by globalisation and transborder data flows.

More specific issues relating to the automated processing of personal data are discussed in guidelines edited by the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, one on the topic of Artificial Intelligence[67] and the other on the processing of personal data in a world of Big Data[68].

The amending protocol is deemed fully compatible with the EU General Data Protection Regulation (GDPR) and the Law Enforcement Directive, and will contribute to convergence towards data protection harmonisation. The European Commission stated that EU wishes to join Convention 108+, and the UN Rapporteur on the right to privacy as recommended to all UN Member States to accede to Convention 108+.

2.2.5 Stakeholders

In the area of electronic forensics and cybercrime at the Council of Europe scale, several main stakeholders need to be identified.

The Convention Committee on Cybercrime (T-CY) is the reporting body of the States Parties to the Budapest Convention. This committee has the same purpose as the Budapest Convention: to facilitate the exchange of information; it participates in the implementation of the Convention and in the review of any changes in the relevant legislation.

The Cybercrime Programme Office of the Council of Europe (C-PROC) is the capacity building body for the implementation of the Convention on Cybercrime. It was established to assist States around the world to meet the challenges of cybercrime and electronic evidence through strong legislation based on the Budapest Convention on Cybercrime. The Office has been assisting countries in implementing the Budapest Convention into national law since 2014, but also participates in the training of judges, prosecutors and police officers, and in the establishment of forensic units.

Each Member State has a CSIRT (Computer Security Incident Response Team) or CERT (Computer Emergency Response Team), which is entitled to respond to cybercrime and cyber-enabled crime, and prevent it. They cooperate in networks at the Council of Europe level and EU level, and have a key role in cooperating with Law enforcement agencies in these matters[69].

Finally, the European Committee on Crime Problems (CDPC) has been responsible since 1958 for directing the Council of Europe's activities in the fight against crime. Through the drafting of conventions, recommendations and reports, it makes proposals for legal cooperation and the improvement of criminal law and procedure.

---

[67] Council of Europe, Directorate General of Human Rights and Rule of Law, and Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Prossessing of Personal Data, "Guidelines on Artificial Intelligence and Data Protection", 25 January 2019 [Online] Available: [https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8].

[68] Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Prossessing of Personal Data, and Directorate General of Human Rights and Rule of Law, "Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data", 23 January 2017 [Online] Available: [https://rm.coe.int/t-pd-2017-1-bigdataguidelines-en/16806f06d0].

[69] ENISA, *An overview on enhancing technical cooperation between CSIRTS and LE*, 2020, [online], available: https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-tools-for-enhancing-cooperation-between-csirts-and-le/@@download/fullReport

In matters of justice, many of the decisions that will be of interest in this topic are made by the European Court of Human Rights (ECHR). This is the judicial body created by the European Convention on Human Rights (EConv.HR), and each state that is party to the Convention has a judge sitting. It is the last instance court concerning the respect of the Convention by the States.

Chapter 3 Encryption, e-evidence and fundamental rights

While encryption is a beneficial tool for citizens in terms of protecting their fundamental rights and freedoms, in particular, the right to privacy, this must be balanced against the needs of law enforcement to ensure national security and public peace. Proportionality, which is often difficult to achieve, must be found between the particular interests and the general interest taking into account the new challenges that digital technology brings to criminal investigations in particular by the blurring of state borders.

3.1 Legality of offences

Sentencing is the very essence of criminal law, and it is only when there is a sentence that the main principles of general criminal law or criminal procedure are applicable. In criminal law, there is a principle summarised in the 19th century Latin phrase: "nullum crimen, nulla Poena sine lege"[70]. This locution reflects the principle of the legality of offences and penalties, according to which there can be no punishment without law and no punishment without a crime.

This principle of the legality of offences and penalties is a fundamental principle of law recognised by all. It is conceptualised in Article 8 of the Universal Declaration of Human Rights, which states that "Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law. At the European level, this principle is found in Article 7 of the European Convention on Human Rights, according to which "1. No one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national or international law at the time when it was committed. Nor shall a heavier penalty be imposed than that which was applicable at the time the offence was committed. 2. This article shall not prejudice the trial and punishment of any person for any act or omission which, at the time when it was committed, was criminal according to the general principles of law recognised by civilised nations".

3.2 Respect for privacy

3.2.1 European framework

Article 8 EConv.HR – Right to respect for private and family life

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[70] "[there is] no crime, no punishment, without law".

Within the right to privacy stands the right to respect for correspondence. This right, in the sense of Article 8 §1 of the EConv.HR, aims to protect the confidentiality of communications in many situations, including data on hard drives[71] but also computer disks[72]. This right to secrecy of correspondence is all the more important with regard to phones, since they have become a singularly important device in the lives of users, becoming indispensable for personal and professional life, but also because of the variety of possible uses. Therefore, any interference with the secrecy of communications must be accompanied by numerous safeguards, especially for correspondence from journalists, lawyers, or other functions with special protection. In any proceedings concerning the use of messages or calls as evidence, the case law of the ECHR considers that **the monitoring of communications and telephone conversations is covered by the notion of privacy, and by the secrecy of correspondence[73]**.

In Europe, any interference with respect for correspondence can only be justified if three conditions are met, as set out in Article 8 §2 of the EConv.HR:

- Interference is provided for by law: although this criterion does not always appear explicitly in the case law, it is essential. In a substantive sense, the law must provide for an infringement for the restriction to be legitimate.
- Interference is inspired by a legitimate aim: the European Court requires that the restrictions should be taken for a legitimate purpose (for example, restrictions on the right to respect for private and family life, home and correspondence (Article 8(2)) may be justified in the interests of public order, public safety, the prevention of crime or the protection of the rights and freedoms of others, or the protection of health or morals)
- Interference is necessary in a democratic society: This is a reference to the central value of European public policy. For a restriction to be necessary, there must be a reasonable proportionality between the restriction and the aim pursued. However, the European Court sometimes leaves a margin to the States, which corresponds to their room for manoeuvre in the respect of rights and in the application of exceptions. This margin of appreciation will be decisive in the scope of the control exercised by the European Court. The Court considers that it is ultimately up to it "to determine whether the purpose and necessity of an infringement of rights by virtue of one or more exceptions provided for to safeguard the public interest are compatible with the Convention".

Interceptions can therefore represent an infringement of privacy and correspondence, and must therefore be based on a clear and detailed law on the subject, especially as the technical procedures that can be used are constantly being improved[74]. When balancing the State's interest in protecting national security through covert surveillance measures against the seriousness of the interference with an applicant's right to privacy, the Court has a certain margin of appreciation in choosing the appropriate means to achieve the legitimate aim of protecting national security. However, there must be adequate and effective safeguards against abuse: the Court takes into account the circumstances of the case, such as the nature, scope and duration of any measures, the reasons for ordering them,

[71] European Court of Humain Rights (ECHR), 27 September 2005, req. N° 50882/99, *Petri Sallinen and others v. Finland*, § 71. [Online] Available: [https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-70283%22]}].

[72] ECHR, 22 May 2008, req N° 65755/01, *Iliya Stefanov v. Bulgaria*, §42. [Online] Available: [https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-86449%22]}].

[73] ECHR, 25 June 1997, req. N° 20605/92, *Halford v. United Kingdom* [Online] Available: [http://hudoc.echr.coe.int/eng?i=001-58039].

[74] ECHR, 24 April 1990, req. N°11801/85, *Krusslin v. France*, §33 [Online] Available: [https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-57626&filename=001-57626.pdf].

the authorities competent to permit, carry out and monitor them, and the type of remedy provided by domestic law[75].

With regard to electronic surveillance and interception, the European Court of Human Rights has developed its case law in relation to the confidentiality of correspondence between a lawyer and his client. In the *Michaud v. France* ruling, the Court held that "Article 8 protects the confidentiality of all 'correspondence' between individuals, and gives greater protection to exchanges between lawyers and their clients. This is justified by the fact that lawyers are entrusted with a fundamental mission in a democratic society: the defence of litigants. A lawyer cannot carry out this fundamental task if he is not able to guarantee to those he defends that their conversations will remain confidential. It is the relationship of trust between them, which is essential for the accomplishment of this mission, that is at stake. In addition, respect for the right of the accused to a fair trial depends indirectly but necessarily on it, particularly insofar as it includes the right of every "accused" not to contribute to his or her own incrimination. This enhanced protection afforded by Article 8 to the confidentiality of exchanges between lawyers and their clients and the reasons for it led the Court to find that, taken from this angle, lawyers' professional secrecy - which, however, is primarily expressed in terms of their obligations - is specifically protected by that provision[76].

Nevertheless, the European Court of Human Rights can sometimes conclude that there has been no violation of Article 8 of the Convention, as in the case of Klass and others v. Germany[77]. The applicants, five German lawyers, complained in particular about German legislation that allowed the authorities to monitor their correspondence and telephone communications without any obligation to inform them subsequently of the measures taken against them. However, the Court held that the German legislature was entitled to regard the interference resulting from the legislation at issue with the exercise of the right enshrined in Article 8 §1 as necessary, in a democratic society, for national security, for the prevention of disorder and for the prevention of criminal offences. In particular, the Court observed that the power of secret surveillance of citizens, which is characteristic of the police state, was tolerable under the Convention only to the extent strictly necessary to safeguard democratic institutions. Noting, however, that democratic societies are nowadays threatened by highly sophisticated forms of espionage and terrorism, so that the State must be able, in order to combat these threats effectively, to monitor secretly the subversive elements operating on its territory, the ECHR considered that the existence of legislative provisions granting powers of secret surveillance of correspondence, mail and telecommunications was, in the face of an exceptional situation, necessary in a democratic society for the protection of national security and/or the maintenance of law and order and the prevention of crime.

3.2.2 National legal frameworks

The secrecy of correspondence, which stems from respect for privacy, is a precious asset in a state governed by the rule of law, which encryption makes it possible to protect even more. Medical data, communications between journalists in countries with laws that are far too restrictive, and digitised commercial transactions are all areas in which the secrecy of correspondence, together with the security and strength of information systems, are fundamental if they are to be used serenely by the

[75] ECHR, 4 December 2015, req. N°47143/06, *Roman Zakharov v. Russia* [Online] Available: [https://hudoc.echr.coe.int/app/conversion/docx/pdf?library=ECHR&id=002-10793&filename=Roman%20Zakharov%20v.%20Russia%20%5BGC%5D.pdf].

[76] ECHR, 6 December 2012, *Michaud v. France* [Online] Available: [https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22002-7327%22%5D%7D].

[77] ECHR, 6 September 1978, req. N° 5029/71, *Klass and others v. Germany* [Online] Available: [https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-57510&filename=001-57510.pdf].

whole population[78]. However, numerous provisions conferring extensive powers to hack and monitor communications (also used to circumvent end-to-end encryption of devices) in different countries have only increased the feeling of widespread surveillance. New interventions are constantly bringing up the issue of backdoors[79], and new "black box" mechanisms are being introduced, even though their results are still too small in relation to the invasion of privacy that these devices have caused[80]. Encryption is also recognised as such by ENISA as an essential element for the secrecy of correspondence[81].

However, it is also recognised that the interception of communications can provide an advantage in solving major investigations. The question here is how such intervention can be considered legitimate from the point of view of national legislation, but also from the point of view of the proportionality of the measure in view of the invasion of privacy that it entails. In this respect, the various partner countries of the Exfiles project have adapted certain national provisions on the confidentiality of correspondence. These provisions are not unified, but have been raised on several occasions in national cases specific to the decryption of devices, the collection of confidential communications, and incidental cases arising from data obtained by operations Encrochat, Sky ECC or An0m.

The following comparative table envisages the main provisions used in these cases and in relation to potential remedies for invasion of privacy.

Table 1: National frameworks for secrecy correspondence

National frameworks for secrecy of correspondence	
France	The French Code of Criminal Procedure allows a search for the purpose of **seizing computer data** to establish the truth about an investigation[82]. Additional restrictions are provided for in order to protect professional secrecy. Another special investigative technique is foreseen, the capture of computer data. This technique was used, for example, in the Encrochat case. The law

[78] Observatoire des libertés et du numérique, Positionning of the Observatoire des libertés et du numérique on « Encryption, security and freedoms", 12 January 2017 [Online] Available: [https://www.laquadrature.net/files/201701_Oln_chiffrementsecuritelibertes.pdf].
French Ministry of Interior, "Answer of the French Ministry of Interior to the written question n°10778", published in the Official Journal of French Republic (*OJFR*) on 18 February 2020, p. 1259. [Online] Available: [https://questions.assemblee-nationale.fr/q15/15-10778QE.htm]. See in particular this part of the answer: "It should be noted, however, that a fourth approach consists of introducing backdoors, i.e., a means of decrypting data in transit between several terminals. However, this development depends on negotiations between the State and the designers of these communication solutions. These negotiations are not made public. Similarly, this approach requires changes to the existing legal framework, which must face up to the divisions of public opinion, opposing the requirements of national security to the defence of public freedoms".

[80] M. Rees, « Renseignement : trois boîtes noires, moins de 10 personnes à risque identifiées en France », *Nextinpact*, 23 August 2019. [Online] Available: [https://www.nextinpact.com/article/29611/108145-renseignement-trois-boites-noires-moins-10-personnes-a-risque-identifiees-en-france].

[81] ENISA, On the free use of cryptographic tools for (self) protection of EU citizens", 20 January 2016. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-position-on-crypto.

[82] French Code of Criminal Procedure, Art. 56 et seq.

National frameworks for secrecy of correspondence	
	provides that it is **possible to set up a device to record, retain, transmit and access data stored in a device, displayed on a screen, entered by typing characters, or exchanged by peripherals**[83]. In practice, this measure makes it possible to obtain the stored data or to capture it in real time using a wide range of techniques. It is necessary to obtain an authorisation from the judge, who is in charge of the control of this investigation technique, and has the possibility to order its interruption[84]. The capture of computer data has an administrative version in the Internal Security Code[85], which provides a **framework for preventive police operations.** As the intrusion into private life is significant, the regime has several guarantees: - Subsidiarity principle: technique used if the information cannot be collected by any other legal means - Validity of authorisation: 30 days for stored data, 60 days for non-stored data - Intervention by intelligence officers - Control by the CNCTR, an independent administrative authority - The Prime Minister's authorisation can only be given after the CNCTR has given its express opinion. Exception in case of absolute urgency, the Prime Minister may grant an authorisation without the prior opinion of the CNCTR.
Netherlands	**The provisions on seizure apply to data contained in telephones.** Seizures and investigations of devices to obtain stored data do not require **prior judicial review or intervention by the public prosecutor**[86]. **If the invasion of privacy is limited**, the Dutch Criminal Procedure Code

[83] *Ibid.* art. 706-102-1.

[84] *Ibid*, art. 706-95-12 and art. 706-95-14.

[85] French Code of internal security, art. L853-2.

[86] Hoge Raad der Nederlanden (HR), ECLI:NL:HR:2017:584 - Hoge Raad, 04-04-2017 / 15/03882. Available: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2017:584.

National frameworks for secrecy of correspondence	
	considers that **the investigation services can legitimately**[87] **collect confidential information** with the traditional seizure provisions. In this case, an *ex post facto* review of the proceedings by the court [88]appears sufficient because of the limited scope of the intrusion by the investigation. The Supreme Court gives examples to distinguish between severe and non-severe infringement[89]: - If the investigation consists only of a small number of specific messages, the investigative measure is considered legitimate. - If the investigation is so extensive that a more or less complete 'picture' is obtained of some aspect of the personal life of the user of the device, the investigation may be considered illegal. The **Netherlands does not yet have a legal regulation that is adapted to the case of data obtained from mobile devices**. Given this lack of regulation, the Supreme Court considers that if the investigation following a seizure involves more than limited intrusion, this investigation would be reasonable[90].
Germany	The monitoring of telecommunications is considered to be an **interference with the secrecy of correspondence according to the German Constitution**, which requires that any interference be regulated by law[91]. However, the German **Code of Criminal Procedure contains a provision allowing for the monitoring of telecommunications**[92]only if : - Certain facts give rise to suspicion that a person has committed

[87] General power of investigators under Art. 94 of the Dutch Code of Criminal Procedure, in conjunction with Art. 95 and 96. See in particular: https://wetten.overheid.nl/BWBR0001903/2021-05-07/#BoekEerste.

[88] Dutch Code of Criminal Procedure, art. 359a. Available: Artikel359aWetboekvanStrafvordering.

[89] HR, 4 April 2017, ECLI:NL:HR:2017:584, *Op. cit.*

[90] Rb. Zeeland-West-Brabant, 31 March 2021, no ECLI:NL:RBZWB:2021:1556. Available online: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBZWB:2021:1556.

[91] German Constitution, "Grundgesetz für die Bundesrepublik Deutschland", Art. 10. https://www.bundestag.de/gg.

[92] German Code of Criminal Procedure, Art. 100a. https://www.gesetze-im-internet.de/stpo/__100a.html

National frameworks for secrecy of correspondence	
	or attempted to commit an offence - The offence is also serious (Article 100a lists the different offences considered serious) - Investigating the facts or determining the location of the individual would be much easier, or futile.
Spain	The **Spanish Constitution** guarantees the secrecy of correspondence, unless a court order[93] is issued. The law limits the use of information technology to guarantee the honour and the private and family life of citizens and the full exercise of their rights[94]. The **Spanish Code of Criminal Procedure** states that any measure limiting the rights to privacy and secrecy of correspondence must be **aimed at a specific punishable act (principle of speciality)**, prohibiting technological investigation measures without an objective basis[95]. According to the judges, **an order to intervene in communications cannot simply be justified by subjective assumptions**, guesses, or the conviction of the existence of a crime. If this practice were sufficient, it would mean that the infringement of the fundamental right to privacy would in practice depend exclusively on the will of the investigator[96]. The evidence must therefore be objective and verifiable, and of such a nature as to make it possible to discover or verify important facts or circumstances of the case[97], or "*indications of criminal responsibility*" [98]<= This position is a translation of the European *Klass* jurisprudence, which requires that wiretapping measures be taken "*only in the presence of indications which give*

[93] Spanish Constitution, art. 18.3.
[94] *Ibid,* art. 18.4
[95] Spanish Code of Criminal Procedure, art. 588 bis a. Available: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=334&modo=2&nota=0.
[96] STS, 86/2018, 19 February 2018. https://vlex.es/vid/704676769.
[97] Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, art. 579. Available: https://www.boe.es/buscar/pdf/1882/BOE-A-1882-6036-consolidado.pdf.
[98] Spanish Constitutional Court, 18 September 2002, 167/2002. Available: http://hj.tribunalconstitucional.es/ca/Resolucion/Show/4703.

National frameworks for secrecy of correspondence	
	rise to suspicion that someone is planning to commit, is committing or has committed certain offences"[99]. It should also be borne in mind that **the constitutional illegitimacy of a wiretap affects subsequent extensions and wiretaps** ordered on the basis of data obtained in the first one[100].
United Kingdom	The framework for regulating interception of communications with mobile phones and other electronic devices (so-called 'equipment interference') in the UK is governed by Part 5 of the "Investigatory Powers Act 2016"[101] (« IPA ») which is supplemented by statutory codes of practice[102]. These codes of practice have an unusual legal status, they enjoy a status similar to that of primary law; thus, violations of its provisions could affect the admissibility of evidence acquired through interception of equipment[103]. Equipment interception warrants are issued by the chief officer of a police area. Judicial oversight is, however, maintained by the requirement, except in cases of emergency, that the decision of a chief officer of a police area to issue a warrant be approved by a judicial commissioner. A warrant will authorise or compel the persons to whom it is addressed to obtain an interception with any "equipment" for the purpose of obtaining communications, equipment data or any other information[104]. It is clear that there is no significant restriction here, moreover, the concept of "communication" is very broad. It includes all files that contain speech, music, sound, visual images "or data of any description", as well as "signals" that transmit anything between people, or between people and things, or that enable any device to function[105].

[99] ECHR, 6 September 1978, Klass and others v. Federal Republic of Germany, No. 5029/71.

[100] Spanish Constitutional Court, 11 September 2006, 253/2006. Available: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/5855

[101] https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

[102] https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice

[103] Investigatory Powers Act 2016, Code of Practice, Equipment Interference (March 2018),

[104] §99(2) Investigatory Powers Act 2016

[105] §135(1) Investigatory Powers Act 2016.

National frameworks for secrecy of correspondence	
	Furthermore, "equipment" is defined very broadly as "any equipment producing electromagnetic, acoustic or other emissions, or any apparatus which can be used in connection with such equipment"[106]. Therefore, these IPA provisions also apply to data contained in telephones, as stated in the Code of Practice[107]. The IPA allows data physically or directly stored in a device to be obtained as admissible evidence, but also data that is physically retrieved, as well as where retrieval software is installed on the device. The second part of the IPA requires those issuing and renewing mandates to take into account several general considerations[108]: - whether what is sought to be obtained by the warrant, authorisation or notice could reasonably be obtained by other less intrusive means, - whether the level of protection to be applied in obtaining information under the warrant, authorisation or advice is higher because of the particular sensitivity of that information, the public interest in the integrity and security of telecommunications systems and postal services, and any other aspect of the public interest in the protection of privacy. In addition, the person issuing a warrant, the Police Commissioner, must justify the application in terms that reflect the grounds for interference with the right to privacy under Article 8(2) of the European Convention on Human Rights. They must consider the warrant necessary to prevent or detect a serious crime and proportionate to the purpose of the interference[109]. With regard to proportionality, the Code of Practice[110] explains that in determining whether this condition is met, the following elements should be taken into account: - The extent of the proposed invasion of privacy in relation to what is being sought;

[106] §135(1) Investigatory Powers Act 2016.

[107] Investigatory Powers Act 2016, Code of Practice, Equipment Interference (March 2018).

[108] See on this subject: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3348711

[109] Investigatory Powers Act 2016 §§106(1)(a)-(b).

[110] Investigatory Powers Act 2016, Code of Practice, Equipment Interference (March 2018).

National frameworks for secrecy of correspondence	
	- How and why the methods to be adopted will cause the least possible interference with the privacy of the individual and others; - Whether the activity is an appropriate use of API and a reasonable way, after considering all reasonable alternatives, to achieve what is sought to be achieved; - What other methods, if any, have not been implemented or have been employed but are deemed insufficient to achieve the operational objectives without the use of the proposed investigative power; - Whether the conduct authorised by the mandate has implications for the privacy and security of other users of equipment and systems, including the Internet, and an explanation of why (if applicable) it is nevertheless proportionate to proceed.
Norway	Two parts of the Norwegian Code of Criminal Procedure deal with the monitoring of communications and possible interceptions[111]. For example, the court may authorise wiretapping for an **offence punishable by 10 years' imprisonment**[112].

These different possibilities of interference can legitimately raise questions in terms of fundamental freedoms, but also concerning the security of the systems used. Numerous laws in recent years have made it possible for investigative and intelligence services to access the computer systems of more or less suspect individuals.

In France, these examples can be seen in the *LOPPSI 2*[113] in criminal matters, and the *law on intelligence* conferring these powers on authorised intelligence services, of which there are currently far too many. In Germany, this possibility is offered in particular by the *Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens*[114], the Netherlands has a hacking power

[111] Norwegian Code of Criminal Procedure, "Straffeprosessloven", ch. 16a and 16b. Available online: https://lovdata.no/dokument/NL/lov/1981-05-22-25/*#&.

[112] *Ibid*, art. 216a. https://lovdata.no/dokument/NL/lov/1981-05-22-25/*#KAPITTEL_4-7.

[113] Law no 2011-267 of 14 March 2011 on the orientation and programming for the performance of internal security *OJFR* no 0062 of 15 March 2011 [Online] Available: [https://www.legifrance.gouv.fr/eli/loi/2011/3/14/IOCX0903274L/jo%2523JORFSCTA000023707348]. This law notably inserted the article 706-102-1 in the Code of Criminal Procedure allowing the possibility to capture computer data. See in particular: REES Marc, "Au Journal officiel, l'encadrement des mouchards de Skype (et assimilés)", *Nextinpact*, 22 July 2015. [Online] Available: https://www.nextinpact.com/article/18703/95893-au-journal-officiel-encadrement-mouchards-skype-et-assimiles.

[114] Law on the more effective and practicable organisation of criminal proceedings of 17 August 2017, Bundesgesetzblatt 2017 Part I no 58 of 23 August 2017, page 3202 [Online] Available: [https://dejure.org/BGBl/2017/BGBl._I_S._3202]. See in particular for a critique of this law : P. Beuth & K. Biermann, "Dein trojanischer Freund und Helfer", *Zeit Online*,

provided for by the *Wet Computercriminaliteit III*, and the United Kingdom has strengthened the investigative powers of its intelligence agencies since *the Investigatory Powers Act 2016*, also conferring these powers on a large number of services[115].

Where mass interception is specifically concerned, the safeguards provided by these national provisions must meet certain new requirements set out by the ECHR.

3.2.3 Focus on the necessary safeguards regarding the mass interception of communications

On 25 May 2021, the European Court of Human Rights handed down two judgments against Sweden[116] and the United Kingdom[117].

In terms of a bulk communications interception regime, Germany, France, the Netherlands and the United Kingdom have formally established such a system, while Norway is reported to have a bill under discussion that would allow for bulk interception of communications[118].

In an attempt to reconcile existing practices with fundamental rights, the European Court clarifies the conditions under which a regime of mass surveillance of electronic communications may be compatible with Articles 8 and 10 EConv.HR[119].

The Court accepts that mass interception is of vital importance to national security[120], but the establishment of such a regime must be accompanied by safeguards against arbitrariness. The Court considers that such a regime **must be framed by end-to-end safeguards,** and a **legal framework assessing the necessity and proportionality of the measures taken must be established**. In the case of the United Kingdom, it was considered that the current regime did not provide these guarantees because:

- Only the Minister authorised surveillance measures, not a body independent of the executive
- The reasons or criteria for the search were not mentioned in the interception requests
- The identifiers used by the intelligence services were not covered by any internal authority
- No specific measures were taken to protect the fundamental rights of journalists

The Court will therefore consider whether the legal framework clearly defines:

- The grounds on which mass interception may be authorised
- The circumstances in which communications can be intercepted
- The procedure for granting a permit
- The process of selection, review and use of intercepted material

---

22 June 2017. [Online] Available: [https://www.zeit.de/digital/datenschutz/2017-06/staatstrojaner-gesetz-bundestag-beschluss/komplettansicht].

[115] V. Garcia, "Le Royaume-Uni instaure la surveillance de masse de sa population", *L'express*, 30 November 2016. [Online] Available: [https://lexpansion.lexpress.fr/high-tech/le-royaume-uni-instaure-la-surveillance-de-masse-de-sa-population_1855595.html].

[116] ECHR, 25 May 2021, no 35252/08, *Centrum för Rättvisa v. Sweden*. [Online] Available: [https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2021/05/3525208.pdf].

[117] ECHR, 25 May 2021, nos 58170/13, 62322/14 and 24960/151, *Big Brother Watch and Others v. United Kingdom*. [Online] Available: [https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2021/05/5817013.pdf].

[118] *Ibid*, §242 and §243.

[119] See in this sense: M-C. Montecler, "La CEDH admet le principe de la surveillance électronique de masse", *Dalloz Actualité*, 28 May 2021. [Online] Available: [https://www.dalloz-actualite.fr/flash/cedh-admet-principe-de-surveillance-electronique-de-masse].

[120] ECHR, 25 May 2021, *Big Brother Watch and Others v. the United Kingdom*, *op. cit.*, § 424.

- Precautions to be taken when communicating these elements to other parties
- Limits on the duration of interception and retention, and the modalities of deletion or destruction
- The procedures and arrangements for supervision by an independent authority of compliance with the guarantees set out above, and the powers of that authority in the event of non-compliance
- Procedures for independent ex post monitoring of compliance with safeguards and the powers of the competent body to deal with cases of non-compliance[121].

3.2.4 National restrictions on the use of encryption

The dilemma between security and freedom also concerns private life. While the use of encryption is generally free but regulated, certain restrictions are added in the form of penalties or aggravating circumstances in the event of the use of encryption in the commission of an offence. These measures are generally intended to compensate for the increased difficulty of obtaining the evidence needed by the investigating authorities.

However, these sanctions are not all the same from one country to another, and in a European Union council, it was pointed out that data encryption hinders the proper conduct of judicial investigations, particularly in the context of the gathering of digital evidence. Similarly, in 2016, France and Germany asked the EU Council to put in place measures to oblige services and operators to cooperate in order to facilitate the extraction of digital data and thus facilitate the obtaining of electronic evidence[122]. This request was made following the various terrorist attacks in France. The French Minister of the Interior therefore wrote a letter in which he stressed the importance of finding effective measures against online communications relating to the glorification of terrorism, violence and the planning of terrorist acts. He stressed that Member States must be able to rely on the cooperation of operators in criminal investigations.

For the European Union, encryption is necessary to protect the fundamental rights and digital security of public authorities, businesses and society in general[123]. A balance must therefore be struck between the protection of fundamental rights through encryption and the need to access electronic evidence in the fight against terrorism and crime.

Table 2: Possible sanctions for using encryption

Possible sanctions for using encryption	
France	The use of encryption is considered an **aggravating circumstance** when it is used to prepare, commit, or facilitate the commission of an offence[124].
Netherlands	No known sanctions

[121] *Ibid. § 361.*

[122] De Maisière, Cazeneuve, "German-French letter concerning cooperation between law enforcement agencies and electronic communication service providers", 4 November 2016. [online] Available: [https://data.consilium.europa.eu/doc/document/ST-14001-2016-INIT/en/pdf].

[123] EU Council Resolution on encryption : Security through encryption and despite encryption, 24 November 2020. [Online] available: [https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/fr/pdf].

[124] French Penal Code, art. 132-79. [Online], Available: [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006417506/].

Possible sanctions for using encryption	
Germany	There is no particular protocol, everything is done on a case-by-case basis and everything depends on the qualification of the offender in terms of handling encryption.
Spain	National legislation establishes a general right for individuals to use data encryption products and services. It requires that providers or users of encryption products or services themselves be licensed or registered in some way and establishes limitations or conditions on the legal import or export of encryption products or services. Article 570 bis of the Penal Code describes an aggravating circumstance for the use of technologies facilitating the commission of organised crime, and higher penalties when the organisation "has advanced technological means of communication [...] which, by virtue of their characteristics, are particularly apt to facilitate the commission of offences or the impunity of the perpetrators of such acts"[125].
United Kingdom	The use of encrypted telephones is considered an **aggravating[126] feature**, and demonstrates a **high level of sophistication[127]** of the criminal operation, which has the effect of raising the importance of the accused in the case and therefore raising the amount of the sentence.
Norway	No known provision

[125]Article 570 bis of the Spanish Penal Code: "Those who promote, form, organise, coordinate or direct a criminal organisation shall be punished by imprisonment for a term of four to eight years if the purpose or object of the organisation is the commission of serious crimes, and by imprisonment for a term of three to six years in all other cases ; and those who actively participate in, belong to, or cooperate financially or in any other way with the organisation, shall be punished by imprisonment for a term of two to five years if the aim or object of the organisation is the commission of serious crimes, and in other cases by imprisonment for a term of three to six years.
For the purposes of this Code, a criminal organisation shall mean a group formed by more than two persons, on a stable basis or for an indefinite period of time, which, in a concerted and coordinated manner, allocates various tasks or functions to itself for the purpose of committing offences". https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

[126] R v Nelson & Markham [2020] EWCA Crim 718. Available: https://vlex.co.uk/vid/r-v-stephanie-nelson-845513719. See: https://www.harewoodlaw.com/news/encrochat-update-the-court-of-appeal, or again: https://sj-law.co.uk/encrypted-phones.

[127] R v English & Read [2020] EWCA Crim 100. Available: https://vlex.co.uk/vid/r-v-dean-english-842824836.

3.3 Proportionality

The principle of proportionality is essential for balancing two fundamental rights. It allows the court to check that the infringement of a fundamental right is not disproportionate.

It is a control which is applied by the European Court of Human Rights but which is now also carried out by the national authorities and even by the Court of Justice of the European Union.

As explained above, any interference with respect for correspondence can only be justified if three conditions set forth in Article 8 §2 of the ECHR are met. One of these conditions were the necessity of interference in a democratic society. For a restriction to be necessary there must be a reasonable proportionality between the restriction and the aim pursued.

Article 5(4) of the Treaty establishing the European Union lay downs the principle of proportionality requiring that "the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties".

The settled case law of the CJEU set forth that "*the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives*"[128]. It therefore "*restricts the authorities in the exercise of their powers by requiring a balance to be struck between the means used and the intended aim (or result reached)*"[129].

Although a margin of appreciation has been left to the Member States by the Court, its main role is to assure that the right to privacy is not interfered unnecessarily. In this respect, ECHR has set forth a proportionality test in its Handyside judgement[130] which consists of four questions[131] :

- Is there a pressing social need for some restriction of the Convention?
- If so, does the particular restriction correspond to this need?
- If so, is it a proportionate response to that need?
- In any case, are the reasons presented by the authorities, relevant and sufficient?

3.4 Subsidiarity

Under the principle of subsidiarity, the European Court of Human Rights will entrust national authorities with the task of ensuring the enjoyment of the rights and freedoms enshrined in the European Convention.

The European Court has implemented the principle of subsidiarity inherent in the European human rights protection mechanism and has recognised the member states' margin of appreciation in the way they apply the rights recognised by the Convention, considering that it: "cannot substitute itself for the competent national authorities, otherwise it would lose sight of the subsidiary nature of the international collective guarantee mechanism established by the Convention. The national authorities remain free to choose the measures they consider appropriate in the fields governed by

[128] Case C-62/14, *Gauweiler (OMT)*, paragraph 67.

[129] Case C-343/09 *Afton Chemical*, paragraph 45; joined cases C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert*, paragraph 74; Cases C-581/10 and C-629/10, *Nelson and Others*, paragraph 71; Case C-283/11, *Sky Österreich*, paragraph 50; and Case C-101/12, *Schaible*, paragraph 29.

[130] *Handyside v. The United Kingdom*, judgment of 07.12.1976.

[131] https://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462513/IPOL-LIBE_ET(2012)462513_EN.pdf

the Convention. The Court's power is limited to the conformity of such measures with the requirements of the Convention".[132]

Similarly, the Court held in Handyside v. the United Kingdom that state systems of human rights guarantees are primary and that the safeguard mechanism established by the Convention is subsidiary to national systems of human rights guarantees[133].

This principle of subsidiarity gives rise to the margin of appreciation left to the states. There are "minimum standards" that must be met by States and the Court leaves a margin of appreciation in regulating and restricting these rights. The intensity of the proportionality control varies in the light of this national margin of appreciation left to the Member States. The Court will rely on certain criteria to determine the extent of the national margin, such as the nature of the right in question and the aim pursued by the restriction. The Court will then compare the rights guaranteed by the Convention that are in conflict in this case and finally it will look at whether there is a common denominator between the Member States or whether, on the contrary, there is not.

Thus, the wider the margin of appreciation, the more flexible the European Court's control will be. On the other hand, the more limited the margin of appreciation left to the Member States, the stricter the control by the European Court will be.

3.5 Right not to self-incriminate

The right against self-incrimination is a recognised "international norm" at the heart of the concept of the right to a fair trial enshrined in Article 6 of the European Convention on Human Rights.

This right has been enshrined by the European Court of Human Rights in two judgments: O'Halloran and Francis v. United Kingdom[134], and Funke v France[135].

These two rulings emphasise the notion that "Every accused person has the right to remain silent and not to contribute to his or her own incrimination".

The right not to self-incriminate applies to criminal proceedings concerning all types of criminal offences, from the simplest to the most complex, as revealed by the European Court's Saunders v. United Kingdom judgment[136]. This judgment emphasises that this right presupposes that the prosecution seeks to establish its case without resorting to evidence obtained by coercion or pressure, in disregard of the accused's wishes.

Thus, the European Court has identified three types of situations that may give rise to a concern that there may be a violation of Article 6 of the European Convention.

---

[132] ECHR, 23 July 1968, no 1474/62 Case "relating to certain aspects of the laws on the use of languages in education in Belgium" v. Belgium. [Online] Available: [https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-57525&filename=001-57525.pdf].

[133] ECHR, 7 December 1976, no 5493/72, *Handyside v The United Kingdom*. [Online] Available: [https://swarb.co.uk/handyside-v-the-united-kingdom-echr-7-dec-1976/].

[134] ECHR, 29 June 2007, nos. 15809/02 and 25624/02, O'Halloran and Francis v. the United Kingdom. [Online] Available: [https://www.echr.coe.int/Documents/Cases_list_2007_ENG.pdf].

[135] ECHR, 25 February 1993, no 10828/84, *Funke v France*. [Online] Available: [https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-62366&filename=001-62366.pdf].

[136] ECHR, 17 December 1996, no 19187/91, *Saunders v. United Kingdom*. [Online] Available: [https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=001-58009&filename=001-58009.pdf&TID=thkbhnilzk].

- The first situation is that of a suspect who, threatened with punishment if he does not testify, either testifies (see the Saunders v. the United Kingdom judgment cited above) or is punished for refusing to do so (Heaney and McGuinness v. Ireland).

- The second situation is where physical or psychological pressure, often in the form of treatment contrary to Article 3 of the Convention, is exerted to obtain a confession or material evidence (Jalloh v. Germany)

- The third situation is the use of subterfuge by the authorities to extract information which they have been unable to obtain through interrogation (Allan v. the United Kingdom).

However, the right not to self-incriminate does not extend to the use in criminal proceedings of data that can be obtained from the accused using coercive powers but which exist independently of the suspect's will, e.g. documents collected under a warrant, breath, blood and urine samples and body tissue samples for DNA analysis (see Saunders v. United Kingdom and O'Halloran and Francis v. United Kingdom).

Why is this an issue?

In the light of various laws, judgments and research findings, it can be considered that the obligation to provide the unlock code of a mobile device does not allow the data to be obtained independently of the suspect's will, which contravenes the right against self-incrimination of Article 6 EConv.HR. Furthermore, access to the data on the suspect's mobile device appears to be a separate operation from its transformation into intelligible data (decryption), since access can be obtained without the suspect's will, but not the unlocking code. This leads to the assumption that the suspect mechanically becomes the interpreter of the data when he provides the unlock code.

In the absence of an obligation to provide the unlocking code, other practices therefore,seem acceptable. The use of limited and proportionate physical coercion, which does not contravene Article 3 of the ECONV.HR, for the purpose of unlocking the suspect's phone through the biometric equipment seems acceptable. The example of forcing a finger on the phone, but also of holding the iris open, has been given by case law and the work of the Koops Committee. It is relevant to consider that these practices come if possible, and prior to the use of decryption techniques that undoubtedly allow to obtain the data necessary for the investigation independently of the suspect's will. Lastly, access to a mobile device using biometrics could be subject to prior authorisation from the judicial order (investigating judge, public prosecutor, etc.).

3.5.1 European framework

The right not to self-incriminate is derived in the case law of the ECHR from Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, concerning the right to a fair trial[137]. This right is also set out in Article 14(3)(g) of the International Covenant on Civil and

[137] ECHR, 25 February 1993, *Funke v. France*, *op. cit.*

Political Rights. By protecting the defendant from undue coercion by the authorities, this right helps to avoid miscarriages of justice and to ensure the right to a fair trial[138].

Principle of European jurisprudence:

In its case law, the ECHR has distinguished 3 distinct situations that may present an undue hardship under Article 6:

- The first situation concerns the suspect who, threatened with sanctions if he does not testify, either testifies[139] or is punished for refusing to do so[140].
- The second situation concerns physical or psychological pressure exerted with the aim of obtaining a confession or material evidence[141].
- The third situation concerns the use of subterfuge to extract information that the authorities have failed to obtain through interrogation[142].

Exception:

An exception has been made in European case law, which has held that this right against self-incrimination does not extend to the use in criminal proceedings of data that can be obtained from the accused by means of coercive powers but which exist independently of the suspect's will143. The Saunders judgment lists some examples of data that exist independently of the suspect's will, such as:

- Documents collected under a warrant
- Breath, blood and urine samples
- Body tissue for DNA analysis

In addition to the above-mentioned "documents collected pursuant to a warrant, breath, blood and urine samples and body tissue samples for DNA analysis".

The grounds for this Saunders judgment was crystallised in Directive 2016/343 of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and the right to be present at trial in criminal proceedings, which states in Article 7 that "*The exercise of the right against self-incrimination shall not prevent the competent authorities from obtaining evidence which may lawfully be obtained by means of lawful coercive measures and which exists independently of the will of the suspected or accused persons*"[144].

---

[138] ECHR, 8 February 1996, no. 18731/91, *John Murray v. the United Kingdom*, § 45. [Online] Available: [https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-62539%22]}].

[139] ECHR, 14 October 2010, no. 1466/07, *Brusco v. France*. [Online] Available: [https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-100969%22]}].

[140] ECHR, 21 December 2000, no. 34720/97, *McGuinness v. Ireland*. [Online] Available: [https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-59097%22]}].

[141] ECHR, 11 July 2006, no. 54810/00, *Jalloh v. Germany*. [Online] Available: [https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-76307%22]}].

[142] ECHR, 5 November 2002, no. 48539/99, *Allan v. United Kingdom*. [Online] Available: [https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-60713%22]}].

[143] ECHR, 17 December 1996, *Saunders v. the United Kingdom*, *op. cit.*

[144] Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 strengthening certain aspects of the presumption of innocence and the right to be present at trial in criminal proceedings, art. 7.3. [Online] Available: [https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0343].

3.5.2 National frameworks

The various national courts have attempted to determine the practical limits of this right in order to determine whether it can, in certain circumstances, apply to the various attempts to unlock mobile devices with the help of the suspect. Some notable situations have emerged from national cases.

The first widespread practice is the obligation to provide national authorities with the unlocking code for mobile devices.

In **France**, refusal to hand over a "secret decryption agreement" (or more concretely, an unlocking code) to the judicial authorities is considered an offence for anyone who has knowledge of the secret decryption agreement[145].

As such, the Constitutional Council declared this provision to be in conformity with the French Constitution[146], considering that this measure is "*not intended to obtain a confession from him or her and does not entail either recognition or presumption of guilt, but only allows the decryption of encrypted data. In addition, the investigation or enquiry must have identified the existence of data processed by the means of encryption that may have been used to prepare, facilitate or commit a crime or offence. Finally, these data, already fixed on a medium, exist independently of the will of the suspected person*"[147]. The case law of the Court of Cassation also rules out the violation of the right not to incriminate oneself for data contained in telephones, while admitting the application of the obligation to decrypt and the qualification of secret encryption agreement to the lock codes of mobile phones[148].

French judges seem to agree that data on a suspect's phone exists independently of the suspect's will, without differentiating between its encrypted or decrypted state, but also that requesting a suspect's phone password in order to exploit it did not violate the right against self-incrimination. This is the position of the Court of Cassation in a judgment of 12 January 2021[149].

This obligation to provide unlocking codes is not present in all countries. For example, the **Netherlands** considers that such an obligation would violate the right against self-incrimination. For this reason, an obligation to decrypt can be addressed to any person who can reasonably be expected to have knowledge of how the data was encrypted[150], but this order cannot be given to the suspect.

[145] French Penal Code, art. 434-15-2.

[146] French Constitutional Court, decision no. 2018-696 QPC of 30 March 2018. [Online] Available: [https://www.conseil-constitutionnel.fr/decision/2018/2018696QPC.htm].

[147] *Ibid*.

[148] French Cour de cassation, Criminal chamber, 12 January 2021, no. 20-84045. [Online] Available: [https://www.legifrance.gouv.fr/juri/id/JURITEXT000043045838?isSuggest=true].

[149] Cass. Crim. 12 January 2021, No. 20-84045. [Online] Available: https://www.legifrance.gouv.fr/juri/id/JURITEXT000043045838?isSuggest=true.

[150] Dutch Code of Criminal Procedure, Art. 126nh. (See also art. 125k, concerning the security of a computer work more generally).

The following table summarises the presence of this type of obligation in the various partner countries

Table 3: Legal obligation for individuals to decrypt

Legal obligation for individuals to decrypt	
France	**A decryption order can be sent to the suspect[151].** It is also possible to ask **third parties who may know the unlocking codes** to decrypt the device.
Netherlands	The decryption order cannot be **addressed to the suspect**[152]. However, it is **possible to address this order to another person** (other than the suspect) who can reasonably be assumed to have knowledge of how this data is encrypted.
Germany	The decryption order cannot be addressed to the suspect. An obligation to cooperate can be put in place when an individual has knowledge of an illegality, or when he or she has information that helps solve a crime. For the accused, however, the right to refuse to testify applies.
Spain	National legislation provides that State authorities may require citizens to cooperate in the decryption of encrypted communications. In Spain, the fifth point of Article 588, which refers to "judicial authorisation" in the Amendment to the Code of Criminal Procedure (LECRIM)1 , establishes that "the authorities and agents in charge of an investigation may order any person with knowledge of the functioning of the computer system or of the measures applied to protect the computer data contained therein to provide the necessary information, provided that this does not entail a disproportionate burden on the person concerned, under penalty of incurring an offence of disobedience". However, this "provision shall not apply to the person sought or prosecuted, to persons exempted from the obligation to testify by reason of kinship and to those who [...] cannot testify by virtue of professional secrecy".

[151] French Code of Criminal Procedure, Art. 434-15-2.

[152] Dutch Code of Criminal Procedure, art. 126nh.

United Kingdom	Where it is not reasonably practicable to obtain the seized data in an intelligible form, the public authority or person with approved authorisation may impose a disclosure obligation in respect of the protected information **on the person it believes to be in possession of the key (the suspect)**[153]. The police can issue this order if : - The unlock code is in the possession of the person notified - Disclosure is necessary to prevent or detect a crime - Disclosure is proportionate to the circumstances - Password protected material cannot be obtained by any reasonable method Failure to comply with a disclosure obligation is punishable by up to two years' imprisonment, a fine or both. In cases involving national security or the indecency of children, the penalty may be up to five years, a fine, or both.
Norway	During a search of computer equipment, **the investigating authorities may order any person dealing with the equipment to provide the information necessary to access the system**[154].

The second practice is the exercise of physical coercion on the individual in order to obtain the mean to unlock the mobile device.

In the Netherlands, the issue of physical restraint for the purpose of unlocking mobile devices has arisen with a cassation appeal to the Supreme Court, which was published on 13 October 2020[155]. A ruling on 9 February 2021[156] followed this previous application

The question was whether the forced use of a suspect's fingerprint to unlock a smartphone used by the suspect for the purpose of gathering evidence constitutes a violation of the right against self-incrimination.

The exercise of the coercive instrument of seizure may imply that, if necessary, by the use of proportionate force, actions are taken to take or retain objects for the purposes of criminal proceedings.

The judgment found that the Dutch power of seizure provided a legal basis for accessing the seized smartphone of the defendant by unlocking it biometrically against his will using his fingerprint. Secondly, the Court held that the application of a very low degree of physical coercion (the finger on

[153] UK Regulation of Investigatory Powers Act 2000, Section 49. [Online] Available: [https://www.legislation.gov.uk/ukpga/2000/23/section/49]. See in particular an article summarising this provision: https://sj-law.co.uk/encrypted-phones.

[154] Straffeprosessloven (Norwegian Criminal Procedure Act), art. 199a. [Online] Available: [https://lovdata.no/lov/1981-05-22-25/§199a].

[155] Dutch Parket bij de Hoge Raad, 13 October 2020, ECLI:NL

[156] Dutch Hoge Raad, 9 February 2021, ECLI:NL:HR:2021:202. [Online] Available: [https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2021:202].

the mobile device) in order to unlock the suspect's device did not violate the right against self-incrimination. The Court, considering that it implied that this physical coercion only resulted in a minor impairment of the accused's physical integrity, nevertheless placed limitations.

In this respect, the conclusions of the public rapporteur preceding the judgment of the Dutch Supreme Court of 9 February 2021 refer to a report on modernising investigations in the digital age by the Koops Committee[157].

In particular, this committee interpreted the Saunders test to mean not only whether something *exists* independently of the suspect's will, but also whether something can be *obtained* independently of the suspect's will. The example is given for the password, which exists in itself independently of the will of the owner of the mobile device, but which cannot be obtained independently of his will.

The committee concluded that biometric access could be imposed on suspects. There would be a difference between cooperation in the form of providing a password, and providing biometric access, since passwords cannot be obtained independently of the suspect's will. **Biometric material would therefore not differ essentially from blood or other bodily substances**, as in the examples mentioned in the ECHR Saunders judgment. As such, the Committee recommended that the legislator include a power for the public prosecutor to order access to a computer system or digital data carrier secured by biometrics.

This is in line with some French positions. In an article dated 7 April 2021, it was considered that body tissues, breath samples, blood samples, etc., were identical regardless of the suspect's intervention. However, this is not the case for encrypted data in a telephone, since the communication of the unlocking code would be broken down into two operations: access to the data on the one hand, and their transformation into intelligible data for the investigator on the other. The suspect would therefore not only be the transmitter of the data (which according to Dutch case law is already considered a violation of the right not to incriminate oneself) but would also mechanically become the interpreter[158]. This calls into question the use in France of the Penal Code to punish the refusal to hand over one's unlocking code[159].

In the alternative, the position of the US Supreme Court provides a rather interesting comparative law perspective in a *Riley*[160] judgment. The Supreme Court distinguishes between the phone as a physical object and the data it contains. This results in a different regime between the examination of the physical characteristics of the phone being freely operable, and the data contained in the phone being given additional protection by the requirement of a warrant. Justice John G. Roberts Jr. said on this issue that:

"Modern 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. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple - get a warrant." [161].

[157] Koops Commission Report, 'Regulering van opsporingsbevoegdheden in een digitale omgeving', 2018. [Online] Available: [https://www.njb.nl/umbraco/uploads/2019/3/Rapport-Commissie-Koops-juni-2018.pdf].

[158] O. Haddad, "Garde à vue: ne dites rien, votre téléphone parlera pour vous", *Dalloz Actualité*, 7 April 2021. [Online] Available: [https://www.dalloz-actualite.fr/node/garde-vue-ne-dites-rien-votre-telephone-parlera-pour-vous#.YK-QqZMzbfY].

[159] French Penal Code, art. 434-15-2.

[160] Supreme Court of the United States, 25 June 2014, *Riley v. California*, 134 S.Ct. 2473, 2493. [Online] Available: [https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf].

[161] *Ibid,* p. 32.

3.5.3 Perspectives and recommendations

This combination of positions leads to two main considerations. On the one hand, the obligation to provide the unlocking code of a mobile device cannot allow data to be obtained independently of the suspect's will, so the Saunders exception does not apply to this practice. Furthermore, accessing the data on the suspect's mobile device is a separate operation from transforming it into intelligible data (decryption), which results in the suspect mechanically becoming the interpreter of that data when he or she provides the unlocking code.

On the other hand, **in the absence of an obligation to provide the unlocking code, other practices therefore seem acceptable**. The use of limited and proportionate physical coercion, which does not contravene Article 3 of the ECONV.HR, for the purpose of unlocking the suspect's phone through the biometric equipment seems acceptable. The example of forcing a finger on the phone, but also of holding the iris open, has been given by case law and the work of the Koops Committee. It is relevant to consider that these practices come if possible, and prior to the use of decryption techniques that undoubtedly allow to obtain the data necessary for the investigation independently of the suspect's will. Lastly, access to a mobile device using biometrics could be subject to prior authorisation from the judicial order (investigating judge, public prosecutor, etc.).

These two considerations lead us to believe **that it would be desirable to harmonise practices at European level**, through additional clarification of the status of the unlocking code and its role in obtaining digital evidence. This harmonisation and clarification of the concepts laid down by the ECHR should in any case not pose additional difficulties for the development of new decryption techniques.

Recommendation

Harmonisation of practices would be desirable at European level, through further clarification of the status of the unlocking code and its role in obtaining digital evidence, but also for the removal of obligations to provide unlocking codes in national legislation, which seem to contravene the fundamental rights of individuals and are not very effective in practice. In any case, this harmonisation and clarification of the concepts laid down by the ECHR should not pose additional difficulties for the development of new methodologies and techniques allowing to bypass encryption.

3.6 Right to a fair trial

This fundamental right derives from concrete rights, like the right to defence, or the right to evidence.

Just as the right against self-incrimination is contained in Article 6§1 of the ECONV.HR, the rights of the defence find their source in Articles 6§1 and 3 of the ECONV.HR, but also in:

- The Universal Declaration of Human Rights (Articles 7, 8, 10 and 11)
- The Charter of Fundamental Rights of the European Union (Article 48)
- The International Covenant on Civil and Political Rights (Article 14)

These rights of defence ensure that in a criminal trial the right to be tried before an independent and impartial tribunal, but also to know the nature of the proceedings against him, **and the contents of his case**.

In the context of the acceptability of evidence obtained abroad, compliance with Article 6 ECONV.HR is equally important. Indeed, evidence obtained illegally by a foreign country in violation of its right

to a fair trial must be taken into account by the criminal court of the country in which the case is being tried, which is not so true for the respect of privacy under Article 8 ECONV.HR. For example, the violation of privacy is not relevant for consideration by the Dutch courts[162].

3.6.1 The right to evidence

There are procedural challenges where it cannot be shown that the evidence was obtained legally. The right to a fair trial generally allows for the protection of individuals of evidence obtained through unfair process by the prosecution, or obtained without a legal basis.

By way of illustration, the Dutch judges consider in a leading case that **exclusion of evidence should follow if the use of the material for evidence constitutes a violation of Article 6** ECONV.HR[163]. From a UK perspective, the *Police and Criminal Evidence Act 1984* has a section excluding disloyal evidence at a criminal trial. Indeed, the Act states that if "*the admission of the evidence* ***would have such an adverse effect on the fairness of the proceedings***"[164], the Court will not admit the evidence.

In contrast, section 56 of *the Investigatory Powers Act 2016* provides for (limited) circumstances in which illegal evidence may be admitted in a criminal trial[165]. In addition, it expressly allows for content obtained directly or physically on a device to be admitted as evidence, and also where software installed on the phone allows for indirect extraction of data[166], a process presumably used in the extraction of communications on Encrochat phones.

This is generally the case in Europe, where European case law considers that **the use of illegally obtained evidence in a criminal trial does not necessarily constitute a violation of the right to a fair trial**. It remains possible that such evidence may lead to an impairment of the fairness of the trial. However, the question will be whether the obtaining of the evidence affected the fairness of the trial. **For example, it has been held that the use of secret recordings obtained unlawfully**, and in violation of Article 8 ECONV.HR, is **not necessarily contrary to the requirements of fairness[167]**.

Particular attention must therefore be paid to the development of techniques that could potentially undermine the right to a fair trial.

3.6.2 The right to defence

Article 6 §3 of the European Convention on Human Rights deals with the rights of the defence and provides that:

---

[162] "Encrochat: juridisch kader onderzoekswensen", *Weening Strafrechtadvocaten*, 27 January 2021, p. 7. [Online] Available: [https://www.strafrechtadvocaten.nl/encrochat-juridisch-kader-onderzoekswensen/].

[163] ECHR, 1 December 2020, no. 46712/15, *Berkman v. Russia*. [Online] Available: [https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-6870993-9213128&filename=Judgments%20of%2001.12.2020.pdf].

[164] Police and Criminal Evidence Act 1984, Section 78, (I). [Online] Available: [https://www.legislation.gov.uk/ukpga/1984/60/section/78/1991-02-01?view=plain#:~:text=(1)In%20any%20proceedings%20the,such%20an%20adverse%20effect%20on].

165 See in particular: "Encrochat Hack: Can Illegally Obtained Evidence Be Used Against You?", *Ashmans Solicitors*, 17 July 2020. https://www.ashmanssolicitors.com/articles/encrochat-hack-can-illegally-obtained-evidence-be-used-against-you/.

166 See in particular: HECKMANN Thibaut, "Droit de l'espace numérique", *FIC*, 15 March 2021. https://observatoire-fic.com/droit-de-lespace-numerique/.

167 ECRH, 14 January 2020, *Stephens v. Malta No. 3*, No. 35989/14, §66. https://laweuro.com/?p=10668.

"Every accused person has the right, in particular, to:

a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the charge against him

(b) To have adequate time and facilities for the preparation of his defence

(c) To defend himself in person or through legal assistance of his own choosing and, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require

(d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him

(e) To have the free assistance of an interpreter if he or she cannot understand or speak the language used in court."

The right to a defence is an integral part of the right to a fair trial guaranteed by the European Convention on Human Rights in criminal matters and applies at all stages of the proceedings.

This article recognises in the first instance the right of the accused to be informed not only of the "cause" of the accusation, i.e. the material facts for which he is being prosecuted and on which the accusation is based, but also of the "nature" of the accusation, i.e. the legal characterisation given to these facts.

A re-characterisation of the facts by the prosecution is possible during the proceedings, but it must allow the accused time to prepare his defence properly.

The accused must have sufficient material to fully understand the charges against him or her in order to properly prepare a defence[168]. For example, there will be sufficient material if the offences charged are sufficiently listed; if the place and date of the offence are indicated; if reference is made to the relevant articles of the criminal code, and if the name of the victim is mentioned[169].

In addition, the accused must be able to organise his or her defence appropriately and without restriction as to the possibility of raising any defence at trial in order to influence the outcome of the proceedings. All of this must, of course, be done within a reasonable period of time (particularly in view of the importance of the proceedings), in a language that the accused understands (which may require the presence of a translator at the hearing) and with access to the documents in the proceedings.

Finally, the accused must be able to exercise the right to a legal recourse available to him or her, and the domestic courts must state the grounds on which they rely with sufficient clarity to allow the accused to exercise a recourse in full knowledge of the facts.

Furthermore, the accused must be given the opportunity to consult a lawyer in order to prepare his or her defence, just as the accused must be given the opportunity to defend himself or herself. Legal aid will be possible if the accused can demonstrate that it is necessary (including financial criteria).

The right of access to a lawyer does not only arise when the person concerned is placed in police custody or questioned by the police, but may also exist in the context of other procedural measures,

[168] ECHR, *Mattoccia c. Italie*, 25 juillet 2000 – see: https://juricaf.org/arret/CONSEILDELEUROPE-COUREUROPEENNEDESDROITSDELHOMME-20000725-2396994

[169] ECHR, *Brozicek c. Italie*, 11 mars 1987 – see: https://juricaf.org/arret/CONSEILDELEUROPE-COUREUROPEENNEDESDROITSDELHOMME-19870311-1096484

for example identification procedures, reconstruction of facts and inspections at the scene, as well as seizure and search operations[170].

However, in France, whether by a judicial police officer under the regime of the flagrante delicto and preliminary investigation or a rogatory commission at the request of the examining magistrate, the perquisition takes the form of a search that can lead to seizures and if the criminal procedure does not explicitly prohibit the presence and assistance of a lawyer during the perquisition, it does not expressly provide for it either. The search regime, which can infringe on fundamental freedoms of property because it constitutes a real invasion of the private life of the persons searched, should be more closely regulated. Article 56(2) of the French Code of Criminal Procedure states that the judicial police officer is "obliged to take all necessary measures in advance to ensure respect for professional secrecy and the rights of the defence". In order to ensure the rights of the defence, should the person subject to a search and seizure not be granted the presence of his lawyer?

In this regard, the French Court of Cassation refused to refer priority questions of constitutionality to the Constitutional Council on the grounds that the assistance of a lawyer is not required during the execution of searches and only becomes necessary if the person concerned is held against his or her will. It added that "searches are procedural acts that can be carried out without the person concerned being under duress"[171].

The lawyer is therefore confronted with a lack of status during searches, leading to many uncertainties for the person searched, particularly with regard to the rights of defence. The police have the obligation to carry out a search in the presence of the person concerned or, in the latter's absence, of two witnesses.

In practice, there is nothing to prevent the person being searched and seized from requesting the presence of his or her lawyer and nothing to authorise the judicial police to oppose this presence. On this subject, the European Court does not impose the presence of a lawyer during a search on the States parties to the Convention, so a standardisation of lawyers, particularly in relation to searches and electronic seizures that are highly invasive of privacy, is essential in the European Union.

Furthermore, the impossibility of making an informed choice of lawyer necessarily undermines the rights of the defence and the fairness of the proceedings as a whole. Thus, in the Beuze v. Belgium judgment of 9 November 2018, the European Court explained that the right of access to a lawyer was intended, in particular: to prevent miscarriages of justice and above all to achieve the aims pursued by Article 6, in particular equality of arms between the accused and the investigating or prosecuting authorities, to provide a counterbalance to the vulnerability of suspects in police custody, to provide an essential safeguard against coercion and ill-treatment of suspects at the hands of the police, and to ensure respect for the right of every accused person not to incriminate himself or herself and to remain silent, which can only be guaranteed - along with the right of access to a lawyer himself or herself - if the accused is properly informed of these rights. In this respect, immediate access to a lawyer who can provide information about procedural rights is likely to prevent any unfairness that might result from the absence of formal notification of these rights.

[170] ECHR, *Ayetullah Ay c. Turquie*, 27 octobre 2020 – see: https://hudoc.echr.coe.int/fre#%7B%22tabview%22:[%22notice%22],%22itemid%22:[%22001-205824%22]%7D

[171] French Cour de cassation, criminelle, Chambre criminelle, 27 avril 2011, 11-90.010, Inédit

Chapter 4 Legal challenges of investigation and evidence

Judicial investigations are increasingly confronted with evidence in electronic form. A new forensic discipline is born: that which deals with digital evidence. Digital tools have invaded our daily life and favoured the commission of criminal offences through them. Nowadays, this discipline is a challenge for the judicial investigators. Even if it is an emerging discipline, forensic investigations are subject to certain rules and principles whose respect is essential to the investigation success. One difficulty is that of the applicable law and the increasing need for cross-border cooperation in terms of sharing evidence.

Even if the establishment of a cooperation framework between state authorities and service providers is necessary to access criminal digital evidence, there is still a lack of comprehensive legal framework specific to electronic evidence. Therefore, the States inevitably rely on their national law during the investigation, causing divergent applications in the partner states. These challenges have become even greater especially with the widespread use of cloud computing, making it even more complicated the issue of jurisdictional interactions for the LEAs, raising many questions about the applicable law.

While even having access to the applicable law remains as another challenge, differences in national legislations and different standards shows a clear need for a comprehensive legal tool for electronic evidence.

4.1 Seizure, interception, copy, write block

In Germany, in accordance with Sections 94 et seq., 102 et seq. and 110 of the German Code of Criminal Procedure the search and seizure of objects on which data is stored (e.g. data are stored (e.g. hard disks or servers), provided that these servers) are possible, provided that these objects constitute evidence in evidence in the context of an investigation.

Similarly, in France, Article 57-1 of the French code of criminal procedure provides that in the context of an investigation in flagrante delicto, the judicial police officer, or the judicial police agent under his responsibility, may access data that relevant to the investigation "by a computer system located on the premises where the search is taking place search is taking place", allowing investigators to take cognisance of data stored in the computer system, but also those stored in the system, but also those stored in another computer system, "where such data system, "where such data is accessible from the original system or available to the from the original system or available to the original system".

In the case of preliminary investigations, Articles 76 and 76-3 of the Code of Criminal Procedure apply[172], this time, access to data may only be granted by decision of the decision of the judge of freedoms and detention for offences and crimes punishable by 3 years or more of imprisonment.

[172] Article 76 of the Code of Criminal Procedure, sub-paragraph 4 "If the needs of the investigation into a crime or offence punishable by a prison sentence of three years or more so require, or if the search for property whose confiscation is provided for in Article 131-21 of the Criminal Code so warrants, the liberty and custody judge of the judicial court may, at the request of the public prosecutor, decide, by a written and reasoned decision, that the operations provided for in this article shall be carried out without the consent of the person in whose home they are carried out".

Furthermore, such data, to which access has been granted under the conditions set out in Article 57-1 of the Code of Criminal Procedure, may be copied onto any medium, seized and placed under seal[173]. In addition, judicial police officers may, "by any means, request any person likely:

1° To be informed of the measures applied to protect the data to which access is permitted in the context of the search;

2° To provide them with the information allowing access to the data mentioned in 1°.

In Spain, the seizure of an electronic device does not also cover the consultation of its contents, which requires express judicial authorisation[174]. On the other hand, "the effective consent of the individual subject will allow the intrusion into his or her right to privacy, since it is up to each individual to limit the scope of the private and family life that he or she reserves for the knowledge of others"[175] and will prevent this scope from being considered violated.

However, there is case law that states that where there is no consent of the owner of the electronic device, nor judicial authorisation, the information contained therein may be accessed provided that it is "motivated by the concurrence of other constitutionally protected legal interests in such a way that an objective and reasonable justification of the interference with the right to privacy can be assessed"[176].

4.2 Mining, extraction

Article 56 of the French Code of Criminal Procedure authorises and defines the conditions for the exploitation of computer media seized in the context of a search. It states that "the judicial police officer may go to the homes of persons who appear to have participated in these offences or to hold evidence, or to any place where property is likely to be found that is subject to confiscation under Article 131-21 of the Criminal Code.

The first paragraph of Article 57-1 of the Code of Criminal Procedure confirms that "judicial police officers or, under their responsibility, judicial police agents may, during a search (...), access data relevant to the investigation in progress (...) via a computer system located on the premises where the search is taking place".

Exploitation may take place immediately at the place of the search. Furthermore, Article 56(5) provides for the possibility of making a copy of computer data in the presence of persons who are present at the search, i.e. either the person concerned or two witnesses present at the scene, in the absence of the person concerned.

---

[173] Article 56 of the Code of Criminal Procedure: "Computer data necessary to establish the truth shall be seized by placing either the physical medium of the data or a copy made in the presence of the persons who are present at the search under legal control".

[174] article 588 a) de la LECrim qui dispose que si la saisie de dispositifs électroniques tels que les ordinateurs, les dispositifs de stockage de masse d'informations, les instruments de communication téléphonique, etc. est prévue avec la pratique d'une perquisition à domicile, "*la résolution du juge d'instruction doit étendre son raisonnement à la justification, le cas échéant, des raisons qui légitiment l'accès des agents autorisés aux informations contenues dans ces dispositifs*".

[175] Spanish Constitutional Tribunal, 1st Chamber, 22 April 2002, Sentencia 83/2002 [Online] Available : [http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4619].

[176] Spanish Suprem Tribunal, Criminal chamber, 4 December 2015, STS 786/2015 [Online] Available : [https://www.poderjudicial.es/search/documento/TS/7602675/abusos%20sexuales/20160219].

The integrity of the copied data will be ensured either by the use of a write blocker at the time of copying, or by the use of any other digital extraction tool that guarantees the non-alteration of the original data for subsequent exploitation.

The data are always examined during the search to ensure that they belong to the person being searched and not to a third party whose data cannot be exploited. The judicial police officer conducting the investigation may therefore examine computer media. The magistrate in charge of directing the investigation may co-submit a specialised service which will have access to the computer media under the same conditions.

The second paragraph of Article 57-1 of the Code of Criminal Procedure allows officers of the judicial police to use computer media seized during a search on the premises of a police or gendarmerie service or unit. All the provisions relating to searches are then applicable. In this context, they may access data relevant to the ongoing investigation and stored in another computer system, if such data is accessible from the original system. As far as possible, this exploitation on police premises must be done when the person concerned is present, i.e. in police custody or at the disposal of the services. Article 56 allows persons present at the time of the search to be retained on the premises if they are likely to provide information on the objects, documents and computer data seized.

The police officer or authorised specialist must first describe the type of equipment to be exploited (whether it is a telephone, a computer, etc.), describe the type of operation to be carried out (data extraction, reconstitution of files, etc.). It should then describe the type of data being analysed (history, multimedia data, encryption etc.).

A copy of the data can be made in accordance with Article 60-3 of the Code of Criminal Procedure. This is particularly preferred for a judicial inquiry or during an investigation.

With regard to data extraction, this is a process of data mining aimed at finding relevant information, which may present some difficulties if the digital medium is locked or broken, for example. Data mining can be partial or complete.

4.3 Integrity of evidence

The security of the data retrieval and reading process is essential to ensure data integrity. Integrity can be defined as "*the property that information or processing has not been altered or destroyed in an unauthorised manner*"[177]. Data integrity is in turn defined as the "*confirmation that the data that have been sent, received or stored are complete and have not been altered*" within the meaning of the European Regulation of 10 March 2004[178]. This element thus makes it possible to guarantee the correct conformity of the elements brought in at the end of an investigation.

4.3.1 The European framework for the integrity of digital evidence

The Council of Europe, in its guidelines of 30 January 2019, established the following fundamental principle with regard to digital evidence: "*Electronic evidence should be evaluated in the same way as other types of evidence, in particular with regard to its admissibility, authenticity, accuracy and*

[177] General interministerial instruction on the protection of secrecy and information concerning national defence and State security no. 1300/SGDN/ PSE/SSD of 25 August 2003. [Online] Available : [https://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/instruction-generale-interministerielle-n-1300-sur-la-protection-du-secret-de-la-defense-nationale/].

178 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, Art. 4, f). [Online] Available : [https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32004R0460].

integrity"[179]. This principle is accompanied by 35 guidelines, including guidelines on the reliability of evidence. Guidelines 19 to 24 state that:

- With regard to reliability, courts should take into account all relevant factors about the source and authenticity of electronic evidence.
- Courts should be aware of the value of trust services in establishing the reliability of electronic evidence.
- To the extent permitted by the national legal system, and subject to the discretion of the court, electronic data should be admitted as evidence, unless one of the parties disputes the authenticity of the data.
- To the extent permitted by the national legal system, and subject to the discretion of the court, electronic data should enjoy a presumption of reliability, provided that the identity of the signatory can be validated and the integrity of the data can be ensured, unless there are reasonable grounds to believe otherwise.
- Where applicable legislation provides special protection for categories of vulnerable persons, that legislation should take precedence over these guidelines.
- To the extent that the national legal system so provides, where a public authority transmits electronic evidence independently of the parties, the content of the evidence shall have evidential value unless it is shown otherwise[180].

These guidelines are designed as a tool for the 47 Member States, and aim at establishing a common framework rather than harmonising national legislation, which only applies insofar as it does not conflict with national legislation[181].

4.3.2 National frameworks for the integrity of evidence

Spain

In Spain, Article 338 of the Code of Criminal Procedure states that "*the instruments, weapons and effects referred to in Article 334 shall be collected in such a way as to guarantee their integrity and the Judge shall agree on their conservation, preservation or handing over to the appropriate body for deposit*"[182].

An important case law from the Supreme Court[183] *in* 2015 dealt with the reliability of conversations held on a social network as evidence. The court insisted that the possibility of manipulation of digital files was a reality, and that "*in such a case, it will be essential to carry out an expert test to identify the true origin of the communication, the identity of the interlocutors and, finally, the integrity of its content*".

---

[179] Council of Europe, 'Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings', CM(2018)169-add1final, 30 January 2019. [Online] Available : [https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902dc9].

[180] *Ibid*.

[181] L. Dargent, 'Council of Europe: guidelines on electronic evidence in civil and administrative proceedings', *Dalloz Actualité*, 12 February 2019. [Online] Available : [https://www.dalloz-actualite.fr/flash/conseil-de-l-europe-lignes-directrices-sur-preuves-electroniques-dans-procedures-civiles-et-ad#results_box].

[182] See in this sense the Spanish Code of Criminal Procedure, [Online] Available : [https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036].

[183] Spanish Suprem Tribunal, 19 May 2015, STS 2047/2015 [Online] Available : [https://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=7390234&links=&optimize=20150527&publicinterface=true].

France

In France, as in other European countries, the freedom of evidence is affirmed[184] and the courts adopt a broad conception of the methods of admission of evidence, which sometimes leads judges to admit evidence provided by the parties from unfair or illegal procedures. This is not the case, however, when the evidence produced is provided by public authorities, which are under a heightened obligation to provide lawful and fair evidence[185].

Furthermore, the probative value of electronic evidence can sometimes be questioned because of doubts about the integrity of the evidence (a problem inherent in the tool used to collect the evidence). Indeed, this evidence can be easily altered, a risk that procedural obligations and the security of the equipment used make it possible to avoid in order to guarantee the authenticity of the elements submitted to the investigation. This type of evidence has the same probative value as electronic writing[186], subject to two cumulative conditions:

- The person from whom it emanates must be duly identified
- The evidence must be established and preserved under conditions that guarantee its integrity

4.3.3 Reliability of the technique used and integrity of evidence

The technical details of the devices used by LEAs are not specifically covered by the legal texts. Judges sometimes state that the method used is irrelevant to the validity of the evidence, as long as it respects the guarantees of reliability. For example, the Amsterdam Court held in 2017 on the issue of the cracking of a suspect's phone password by the *Netherlands Forensic Institute* (NFI), that **since the method itself had no influence on the content of the messages,** the **evidence was valid as long as there was no doubt as to the accuracy of the messages** brought as evidence before the courts[187].

On the other hand, if the technical specificities of the method used are not really taken into account, the fact remains that the method must be accompanied by guarantees of the traceability of actions and the reliability of the process, in order to be integrated without difficulty into the Chain of Custody.

Indeed, the consequences of unreliability in the technique used can be considerable. Denmark is an example: In 2019, more than 10,000 investigations that relied on phone location data were challenged, as a problem in the data collection was demonstrated, notably concerning time stamping[188]. Electronic time stamping is a means of ensuring data integrity, defined by the eIDAS Regulation as "*data in electronic form linking other data in electronic form at a specific point in time, providing evidence that the latter data existed at that point in time*"[189]. If the principle of freedom of

[184] French Code of Criminal Procedure, art 427.

[185] French Cour de cassation, Criminal chamber, 11 May 2006, nº 05-84.837, Bull. crim. nº 132. [Online] Available : [https://www.legifrance.gouv.fr/juri/id/JURITEXT000007069886/].

[186] French Civil Code, art. 1366.

[187] Dutch Rechtbank Amsterdam, 20 July 2017, no. 13/997096-15, [Online] Available : [https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2017:5132].

[188] "Denmark: geolocation at the origin of thousands of judicial errors?", *Le Point*, 24 August 2019. [Online] Available : [https://www.lepoint.fr/high-tech-internet/danemark-la-geolocalisation-a-l-origine-de-milliers-d-erreurs-judiciaires-24-08-2019-2331426_47.php].

[189] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Art 3, 33°. [Online] Available : [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG].

evidence is generally recognised in European countries, allowing the judge to rely on his or her own conviction to decide on an investigation, the integrity of this digital evidence must still be admitted.

The data obtained by a tool must therefore provide the usual guarantees of integrity, but the tool itself must be considered reliable. This perspective is all the more important for tools for decrypting and extracting data from mobile devices as recent news has revealed various flaws in the tools used by public authorities.

On 21 April 2021, a blog post from the Signal website highlighted some vulnerabilities in Cellebrite's tools[190]. Cellebrite creates software to automate the physical extraction and indexing of data from mobile devices. They have created two pieces of software that are widely used in criminal investigations: UFED and Physical Analyzer.

UFED is used to create a backup of the mobile device on the computer using UFED, while Physical Analyzer is used to analyse the files in the backup to display the data in a searchable form. Currently, more than 2,000 LEAs are reported to be using such tools, including both rule of law states and other governments that are more repressive of fundamental freedoms[191].

In its blog post, Signal performed a Proof of Concept, showing that it was possible to inject arbitrary code into the machine, and that almost any type of code could be injected. Since the extracted data is generated and controlled by the device's applications, an application could (according to Signal) lie to Cellebrite, as the extraction software has no mechanism to verify the information it receives. The security of these tools is therefore presented as lacking.

Whether or not these vulnerabilities have been exploited by some services in practice, the mere prospect of such a vulnerability could pose difficulties in investigations in terms of the reliability of evidence from these tools. In order to minimise this risk as much as possible, provision should be made for the auditability of new tools under development by specialised and independent services.

4.4 Retrieving of unencrypted data

The technical means used by criminals to make it impossible to access the content of their mobile phone exchanges complicates the work of the investigation teams, which is faced with encrypted data that is difficult to extract and exploit. This is even difficult when there is a very large mass of data.

Confronted with this type of challenge, investigative services are trying to equip themselves with tools to deal with encryption. However, the legislator has given LEAs the prerogative of deciphering the data.

Some states have included measures in their legal frameworks that directly address this issue when an encrypted device is seized. the question of the legality of these methods arises, of course, as they contravene fundamental principles of human rights and freedoms. In view of this, the legal protection afforded to these methods must be explored.

[190] MoxieO, "Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective", *Signal*, 21 April 2021. [Online] Available : [https://signal.org/blog/cellebrite-vulnerabilities/].

[191] R. Pfefferkorn, "I have a lot to say about Signal's Cellebrite hack", *Stanford Law School Blog*, 12 May 2021. [Online] Available : [https://cyberlaw.stanford.edu/blog/2021/05/i-have-lot-say-about-signal%E2%80%99s-cellebrite-hack].

4.4.1 Direct extraction

Table 4: Data decryption procedure

Data decryption procedure	
France	A Technical Assistance Centre (TAC) has been set up, which investigative services can use when an investigation concerns an offence punishable by at least two years' imprisonment[192].
Netherlands	Dutch law provides for the possibility for the public prosecutor to **order an encryption service provider to provide the data stored on their servers**[193], but the problem of territoriality may arise when the data is abroad. This provision is not suitable for end-to-end encryption, as the service provider itself does not have readable access to the data. For this reason, the Rotterdam Court recognised the possibility of accessing end-to-end encrypted data through a connection to the user's account (the case in question concerned Telegram), provided that it is not possible to obtain the data in a readable format in any other way[194]**.** An additional power for the **intelligence services** is found in the *Intelligence and Security Services Act*, which **allows the authorised services to decrypt communications**[195].
Germany	The use of classified software to intercept telecommunications before they are encrypted is not subject to specific rules, although the strict requirements for preventive measures in § 20k BKAG should a fortiori apply to investigative measures of the same nature[196]. Section 20k of the German Code of Criminal

[192] Code of Criminal Procedure, Art. 230-1, para. 3.

[193] Dutch Code of Criminal Procedure, art. 126 [Online] Available: [https://wetten.overheid.nl/jci1.3:c:BWBR0001903&boek=Eerste&titeldeel=IVA&afdeling=Negende&artikel=126ng&z=2021-05-07&g=2021-05-07].

[194] Rechtbank Rotterdam, 22 February 2019, no. 10/960268-18. [Online] Available: [https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBROT:2019:2712].

[195] Intelligence and Security Services Act 2017 "Wet op de inlichtingen- en veiligheidsdiensten 2017", art. 48 [Online] Available: [https://wetten.overheid.nl/jci1.3:c:BWBR0039896&hoofdstuk=3&paragraaf=3.2&sub-paragraaf=3.2.5&sub-paragraaf=3.2.5.6&sub-paragraaf=3.2.5.6.3&z=2020-01-01&g=2020-01-01].

[196] The Collection of Electronic Evidence in Germany: A Spotlight on Recent Legal Developments and Court Rulings [Online] Available : https://link.springer.com/chapter/10.1007%2F978-981-10-5038-1_1

Data decryption procedure	
	Procedure[197] provides that the Federal Criminal Police Office may intervene in computer systems used with technical means without the owner's knowledge and collect data from them if certain facts justify the assumption that there is a danger to a person's life or freedom or threatens the existence of the state.
Spain	On 14 March 2011, the Criminal Procedure Code was amended to give additional powers to the authorities investigating terrorist attacks. These amendments include: • the power to seize documents relevant to an investigation (including the conversion and transfer of computer data) • decryption of protected computer data, • digital covert operation, • interception of computer data (including images), • tapping and interception of other communications.
United Kingdom	The UK Government has put provisions in place to ensure that it receives information in a decrypted format. To ensure that, it has been foreseen to serve a technical capability notice ("TCN"), imposing on communication service providers certain obligations, including to decrypt the communication or data. As per the Equipment Interference Code of Practice article 8.1. telecommunications operatorsay be required "to provide assistance in giving effect to interception, equipment interference and bulk acquisition warrants and notices or authorisations for the acquisition of communications data. The purpose of maintaining a technical capability is to ensure that, when a warrant, authorisation or notice is served, companies can give effect to it securely and quickly." Article 8.6 « An obligation imposed by a technical capability notice on a telecommunications operator to remove encryption does not require the provider to remove encryption per se. Rather, it may require that operator to

[197] Article 20k of the German Code of criminal procédure [Online] Available : https://dejure-org.translate.goog/gesetze/BKAG/20k.html?_x_tr_sl=de&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=sc

Data decryption procedure	
	maintain the capability to remove encryption when subsequently served with a warrant, notice or authorisation. ». Article 8.7. « As with any other obligation contained in a technical capability notice, an obligation to remove encryption may only be imposed where it is reasonably practicable for the relevant telecommunications operator to comply with it. A decision regarding what is reasonably practicable will depend on the particular circumstances of the case, recognising that what is reasonably practicable for one telecommunications operator may not be for another. Such an obligation may only relate to electronic protections that the company has itself applied to material or where those protections have been applied on behalf of that telecommunications operator and not to encryption applied by any other party. References to protections applied on behalf of the telecommunications operator include circumstances where the telecommunications operator has contracted a third party to apply electronic protections to a telecommunications service provided by that telecommunications operator to their customers. » Article 8.8. « While an obligation to remove encryption may only relate to protections applied by or on behalf of the company on whom the obligation is placed, an equipment interference warrant may require a telecommunications operator to take such steps as are reasonably practicable to take to give effect to it. This will include, where applicable, providing material in an intelligible form. An example of such circumstances might be where a telecommunications operator removes encryption from material for their own business reasons. »
Norway	Under a section of the Norwegian Code of Criminal Procedure[198], the police are **allowed to break or bypass the protection of computer systems**. They may use technical devices and computer programs to assist in reading the data. A limitation is placed in the same section, requiring that data is not captured unnecessarily.

[198] Norwegian Code of Criminal Procedure, art. 216. Available: https://lovdata.no/dokument/NL/lov/1981-05-22-25/*#KAPITTEL_4-10.

4.4.2 Legal protection of methods used by law enforcement

Disclosure of the processes used by law enforcement will inevitably hamper investigations and thus give criminals the advantage, allowing them to find a way around these techniques to continue encrypting their exchanges. In order to protect these methods, the protection of State processes used for the extraction of encrypted data is paramount to effective investigations.

In this respect, it is important to have the legislative tools for the protection of state resources. The first means of protection that may come to mind is the protection granted by intellectual property rights, which can applie to content and processes created by the administration.

In general, the owner of an intellectual property right may prevent the reproduction, representation, imitation or exploitation of all or part of an intellectual property right without his or her authorisation, subject to the exceptions specified in the Intellectual Property Code (IPC). Intellectual property is divided into two main branches which provide different conditions for protection: (i) industrial property, including trademarks, patents and designs, and (ii) literary and artistic property, including creations such as literary, musical and graphic works, but also software and databases.

The conditions for protection differ between these two categories. For literary and artistic property, the creation must be original. The presence of originality is not easy to achieve and is assessed by the judge on a case-by-case basis, in the event of a dispute. On the other hand, industrial property rights require a registration formality. The State can always benefit from this protection conferred by intellectual property law for its creations and contents provided that they meet the conditions of protection provided by the IPC and by case law. **However, the provisions of the Intellectual Property Code do not constitute a legitimate reason for not disclosing this information to the information before the judicial authorities**.

On the other hand, national defence can be argued to determine the classification of information and evidence and thus be considered as a legitimate reason that prevents the disclosure of those processes used during the clarification of encrypted data in the course of legal proceedings.

In France, for example, State resources subject to national defence secrecy, State security, public security and personal security cannot be disclosed because of their content[199]. They may not be disclosed before the judicial authorities either. Apart from exceptions, only the result of the technique, in this case the decrypted data, will be produced in the judicial file.

In other words, national defence information is kept secret and is not disclosed to the accused and the judicial authorities in the name of national security. This practice inevitably affects the rights of the defence and the right to a fair trial. Another problem with this is that a very broad scope of the notion of 'national security' may lead to the violation of fundamental rights of individuals and create a risk that LEAs act in an arbitrary manner.

These issues will be further analysed in a comparative study of legal frameworks, interpretations by national courts in the partner countries of this project as well as in European courts in deliverable no. 2.3 of the EXFILES project, dedicated to the admissibility of evidence in court.

4.4.3 Remote access on the cloud

In the current use of smartphones, most communication, document exchange and backup activities are done through the use of a cloud, i.e. servers distant from the device. Often, the case arises where these servers are not located in the country of use of the device, as they are centralised in another country of the European Union, or even in a third country outside the Union.

[199] Article L. 311-5, 2nd paragraph of the French Code of relations between the public and the administration ("CRPA").

The challenges of recovering digital evidence in foreign countries are of particular importance for investigations. A European Commission recommendation of 2019 recalled that fifty percent of investigations require the seizure of digital evidence stored on different servers located in other states[200]. In order to obtain this evidence, it may be necessary to resort to mutual legal assistance treaties (MLAT). Because of the many issues surrounding this recovery, a comprehensive law on cross-border access to digital evidence is being developed, notably with the *Second additional protocol to the Convention on Cybercrime*, adopted on November 2021, and the draft "E-evidence" regulation[201].

Within the EU, this problem therefore depends mainly on the cooperation mechanisms between the Member States and the possibility to require service providers to hand over evidences; these issues are dealt with in section 4.7 of this document. The issue of cooperation of service providers is also dealt with in section 5.4 from a data protection perspective.

4.5 National procedures in obtaining digital evidence

The procedures for obtaining access to electronic evidence may vary from jurisdiction to another. In cybercrime and cyber-enabled crime, investigations rarely end at the borders of a Member State, and cross-border investigations are necessary. In this case, judicial authorities are confronted with the differences between the legal frameworks of the different countries, which can cause problems in the admission of evidence, even in the case of a joint investigation. The Encrochat case is a good example of this, and will serve to explain this issue.

4.5.1 The Encrochat case

4.5.1.1 Background of the case

Encrypted smartphones with the trade name Encrochat coupled with a specific messaging service were sold around the world to ensure criminal acts, with 90% of its users being connected to the criminal world[202]. An investigation unit was mobilised, and a technical device was used to break the encryption of Encrochat phones. The operation was codenamed "Emma 95" in France and "26Lemont" in the Netherlands.

The internal development of the case is still for the most part covered by national secrecy, but it is likely that the specialised unit of 60 French gendarmes accessed the Encrochat servers, hosted in France by the company OVH, in order to force the installation of software allowing the surveillance of communications before their encryption[203].

[200] European Commission, "Recommendation for a Council decision authorising the opening negotiations in view of 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", COM(2019)70 final, 5 February 2019, p.1.

[201] European Commission, Proposal for a Regulation of the European Parliament and of the Council on European orders for the production and preservation of electronic evidence in criminal matters, COM(2018) 225 final, 17 April 2018.

[202] FOLLOROU Jacques, UNTERSINGER Martin,"Le réseau crypté EncroChat infiltré par les polices européennes : " C'est comme si nous étions à la table des criminels "', *Le monde*, 3 July 2020. [Online] Available: [https://www.lemonde.fr/international/article/2020/07/03/c-est-comme-si-nous-etions-a-la-table-des-criminels-comment-les-polices-europeennes-ont-penetre-le-reseau-crypte-encrochat_6045024_3210.html].

[203] THIERRY Gabriel, "l'infiltration des smartphones Encrochat décapite la criminalité européenne'', *Lessor*, 25 June 2021. [Online] Available: [https://lessor.org/societe/linfiltration-des-smartphones-encrochat-decapite-la-criminalite-europeenne/].

The success of this operation has had a significant impact in many countries, including the UK, where the NCA reported in July 2020 that it had launched investigations using EncroChat data, leading to the arrest of 746 people, £54 million in cash, 77 firearms and 2 tonnes of drugs. Other notable catches have been made in different countries using EncroChat data, such as the discovery of a torture room in shipping containers in the Netherlands, or the seizure of 11 tons of cocaine by the Belgian police.

4.5.1.2 Legal grounds of the Encrochat case

The French investigation was conducted in accordance with the legal rules applicable in France. The special investigative technique used was the **capture of computer data**, as provided for in Article 706-102-1 of the French Code of Criminal Procedure[204], which states

***"**A **technical device** may be used to **access, record, store and transmit computer data anywhere, without the consent of the persons concerned, as stored in a computer system, as displayed on a screen for the user of an automated data processing system, as entered by the user by typing characters or as received and transmitted by peripheral devices**. (…)* »

This measure, as well as other special investigative techniques, is subject to a specific framework in France. Thus, these investigative techniques are authorised during the investigation by the liberty and custody judge at the request of the public prosecutor, and during the investigation by the investigating judge, following the opinion of the public prosecutor[205]. In addition, the magistrate who authorised this measure carries out a review. The latter may order their interruption at any time[206].

The technical device used in the Encrochat case is covered by national secrecy, the disclosure of which is punishable under the criminal code[207]. However, some clarifications have been made, notably in a report published by Eurojust, the European Union's judicial cooperation unit[208]:

- A technical device through which the communications of many users of the communication solution involved in criminal activities and of facilitators of this solution deliberately made available to criminal organisations could be accessed in an unencrypted way
- A technical device for which it was prescribed "the use of State resources subject to national defence secrecy" (Art. 706-102-1 of the French Code of Criminal Procedure)
- A device whose design and operation are covered by national defence secrecy, but which was received and deployed by a service authorised by law to do so, the Gendarmerie Nationale's Central Criminal Intelligence Service (SCRC) of the Gendarmerie Nationale's Judicial Pole (PJGN) in application of Article D15-1-6 of the Code of Criminal Procedure.

Concerning the lack of proportionality that has been alleged towards law enforcement, seems that the interception of messages from several thousand users can be considered as a highly disproportionate measure. Especially since according to the European case law *Big Brother Watch v. United Kingdom*, mass interception **must be proportionate to the aim[209]**. Arresting a group of criminals was the legitimate goal of the investigators, and the courts may have to rule on proportionality in this case.

---

[204] Art. 706-102-1 of the French Code de procédure pénale.

[205] Art. 706-95-12 of the French Code de procédure pénale.

[206] Art. 706-95-14 of the French Code de procédure pénale.

[207] Art. 413-9 and 413-10 of the French Code pénal.

[208] Eurojust, "The Encrochat investigation in France", 2 July 2020. [Online] Available: [https://www.eurojust.europa.eu/sites/default/files/Press/2020-07-02_EncroChat-investigation-in-France_FR.pdf].

[209] ECHR, 25 May 2021, *Big Brother Watch and others v. United Kingdom, no. 58170/13, 62322/14 and 24960/15.* [Online] Available: [https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2021/05/5817013.pdf].

4.5.2 National procedures

The outcome of the Encrochat case has tested the adaptation of different national legal systems and has led to numerous appeals in different countries. This provides an opportunity to learn more about the legal means and possibilities of admitting such evidence obtained in the context of a case such as Encrochat. This case is an interesting point in the convergence of legal means and the admissibility of evidence, as many countries have had to assess the admissibility of evidence from Operation Encrochat. While some countries such as France and the Netherlands have accepted this evidence, the situation has been different in other countries. For example, a Swedish court rejected the Encrochat[210] evidence, while the UK restricted its acceptance of evidence.

4.5.2.1 United-Kingdom's framework

The UK judiciary was asked to give a judgment questioning the admissibility of evidence from Operation Encrochat in a case called *"R v A, B, D, & C [2021] EWCA Crim 128*". [211]which was commented on by Alexandra Wilson among others[212].

The Investigatory Powers Act 2016[213] sets out the lawful practice of surveillance, interception and investigation by the UK investigative services. A difference in regime and admissibility of evidence exists depending on whether the interception of messages was carried out **at the time of transmission, or when they are stored in the system**.

Indeed, section 56(i) of the 2016 *Act* provides an **initial guarantee of secrecy of correspondence, but also an exception to allow for a wide range of evidence to be used in court**:

" *No evidence may be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings or Inquiries Act proceedings which (in any manner)*

(a)discloses, in circumstances from which its origin in interception-related conduct may be inferred

- *(i)any content of an intercepted communication, or*
- *(ii)any secondary data obtained from a communication, or*

(b)tends to suggest that any interception-related conduct has or may have occurred or may be going to occur." [214]

This protection for individuals is subject to exceptions found in Schedule 3 of the 2016 *Act*, referring to a section 6 which provides that an interception of communications is only possible if it is carried out on a communication stored in a telecommunications system and in accordance with an *equipment interference warrant*[215].

---

[210] "Zweeds hof verwerpt EncroChat-bewijs," *Crimesite*, 12 May 2021. [Online] Available: [https://www.crimesite.nl/zweeds-hof-verwerpt-encrochat-bewijs/].

[211] R v A, B, D, & C [2021] EWCA Crim 128. [Online] Available: [https://www.bailii.org/ew/cases/EWCA/Crim/2021/128.html].

[212] WILSON Alexandra, "Alexandra Wilson examines the Court of Appeal 'Encrochat' judgment: A, B, D & C v Regina [2021] EWCA Crim 128", *5SAH,* 25 March 2021. [Online] Available: [https://www.5sah.co.uk/knowledge-hub/articles/2021-03-25/alexandra-wilson-examines-the-court-of-appeal-encrochat-judgment-a-b-d-and-c-v-regina-2021-ewca-crim-128].

[213] Investigatory Powers Act 2016. [Online] Available: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

[214] Investigatory Powers Act 2016, Section 56 (1). https://www.legislation.gov.uk/ukpga/2016/25/section/56/enacted

[215] Investigatory Powers Act 2016, section 3 (1) (c) (i). [Online] Available: [https://www.legislation.gov.uk/ukpga/2016/25/section/6/enacted].

Specifically, this article allows for the **data physically or directly stored in a device, but also physically retrieved data, as well as when retrieval software is installed on the device, to be** obtained as **admissible evidence**.

In the above-mentioned EWCA Crim 128 judgment, the judges recognised that the data obtained by the French and Dutch investigative services did not constitute an interception during the sending (which is prohibited by UK law[216]), but a direct intervention on data stored in the device, which therefore does not contravene the provisions of the *Investigatory Powers Act 2016*. According to the British judges, the French software retrieved the message before it was sent, and the same was true for the metadata obtained, which were only present in the phone's memory[217]. As a result of this case law, all challenges to the admissibility of the evidence obtained from Encrochat were dismissed.

4.5.2.2 Dutch national framework

The principle of *legality of arms* implies that the defence must be able to verify the legality of the way in which the evidence was obtained.

In the Netherlands, a provision comparable to the grounds used in the French investigation exists. It is an article 126uba Sv, of the Dutch Code of Criminal Procedure. It is on the basis of this article that the Encrochat data were processed in the Netherlands.

Among other things, this provision allows for **the interception of communications where a certain degree of suspicion against a suspect is present**[218]. Certain safeguards are provided for, as this article can only be applied in cases of reasonable suspicion of crimes, and where the interests of the investigation urgently require the use of this technique[219].

Once the computer system has been penetrated, another provision, article 126t of the Dutch Code of Criminal Procedure, must be applied. It allows **the recording of confidential communications[220].** This measure can only be applied if there is a reasonable suspicion of involvement in organised crime.

According to the link between these two articles, only communications from Encrochat users who plan or commit crimes in an organised context can be intercepted[221].

In the appeals before the Dutch courts, under the principle of mutual trust, the Dutch courts considered that **their review was limited to ensuring that the results of the investigation did not violate the right to a fair trial** under Article 6 ECONV.HR, and **that it was not for them to verify how the investigation was conducted in accordance with the relevant French legal rules. Nor was** it **for the judge to verify whether the French investigative acts were carried out in violation of the privacy of the suspects**[222].

---

[216] Investigatory Powers Act 2016, section 3.

[217] HECKMANN Thibaut, "Droit de l'espace numérique", *op. cit*.

[218] Dutch Code of Criminal Procedure, art. 126uba. [Online] Available: [https://wetten.overheid.nl/jci1.3:c:BWBR0001903&boek=Eerste&titeldeel=V&artikel=126uba&z=2021-05-07&g=2021-05-07].

[219] "Encrochat: juridisch kader onderzoekswensen", *Weening Strafrechtadvocaten*, 27 January 2021, p. 24. [Online] Available: [https://www.strafrechtadvocaten.nl/encrochat-juridisch-kader-onderzoekswensen/].

[220] Dutch Code of Criminal Procedure, art. 126t. [Online] Available: [https://wetten.overheid.nl/jci1.3:c:BWBR0001903&boek=Eerste&titeldeel=V&artikel=126t&z=2021-05-07&g=2021-05-07].

[221] Encrochat: juridisch kader onderzoekswensen", *Weening Strafrechtadvocaten*, *op. cit.,* p. 24.

Dutch Code of Criminal Procedure, art. 126t. Available online:

[222] See e.g. Rechtbank Amsterdam, 18 December 2020. [Online] Available:, [https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2020:6443], but also Rechtbank Oost-Brabant,

4.5.2.3 German national framework

According to the provisions of the German Code of Criminal Procedure[223], the search and seizure of objects on which data are stored is possible, **provided that these objects constitute evidence** in an investigation.

In the context of interception of telecommunications under Sections 100a and 100b of the Criminal Procedure Code, the collection of traffic/content data in real time is possible. However, this presupposes that a serious criminal offence listed in Article 100a (2) of the Code is suspected and that interception under Article 100b has been ordered by the court in accordance with the usual procedure. Traffic data, such as the numbers or identifiers of the connections concerned or of the terminals, as well as location data of a mobile phone can also be obtained under Article 100g of the CPC. This is done only when a criminal offence of significant importance, even in an isolated case (including in particular the offences listed in Article 100a(2) of the Code of Criminal Procedure, or a criminal offence using telecommunications), has been committed.

If the measure refers to traffic data that must be stored by telecommunication companies for a certain period of time in accordance with the Data Retention Obligation Act, which entered into force on 18 December 2015, collection is only permitted in the case of particularly serious criminal offences within the meaning of the Data Protection Act. Particularly serious criminal offences within the meaning of the offences listed in Section 100g (2) of the above-mentioned Code. In all cases of traffic data collection, a court order is normally required. The collection of traffic data may be done by means of a court order.

4.6 Distinction between preventive and investigative measures

Security measures are preventive measures; they deprive or restrict freedom or rights. These measures, unlike investigative measures, are not based on the commission of an offence but solely on the observation of the supposed dangerousness of an individual.

Preventive measures known as security measures can be judicial (ban on residence, registration in the FIJAIS, etc.) or administrative (closure of establishment).

However, security measures are not considered as criminal convictions within the meaning of Article 7 of the European Convention on Human Rights[224].

In the field of counter-terrorism and intelligence, administrative police measures were taken following the attacks in France in 2015. Initially, there was the law of 30 October 2017, known as the SILT law strengthening internal security and the fight against terrorism, then more recently the law of 30 July 2021 on the prevention of acts of terrorism and intelligence[225], which perpetuates and adapts certain counter-terrorism measures tested since 2017.

---

4 May 2021, ECLI:NL:RBOBR:2021:2234, [https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBOBR:2021:2234].

[223] German Code of Criminal Procedure, §§ 94 ff. concerning seizure, but also 102 ff. and 110 concerning the examination of electronic data. [Online] Available: [https://www.gesetze-im-internet.de/stpo/].

[224] ECHR 1 July 1961, *Lawless v. Ireland, § 19: "*The Irish Government detained the applicant solely for the purpose of preventing him from engaging in activities prejudicial to the maintenance of public peace and order or the security of the State. This detention, which constitutes a preventive measure, cannot be regarded as resulting from a criminal conviction within the meaning of Article 7".

[225] LOI n° 2021-998 of the 30 Juy 2021 on the prevention of terrorist acts and intelligence. [Online] Available: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043876100

With regard to the prevention of acts of terrorism, the law of 30 July 2021 in France has in particular clarified the issue of search and seizure. If the search reveals the existence of documents or data that are particularly serious for security and public order, the data and computer system may be seized or copied. But the law has modified Article L229-5 of the Internal Security Code[226]. Indeed, it has included a new paragraph, paragraph 2, which states that if the occupant obstructs access to data relating to a particularly serious threat to security and public order, the medium may be seized.

However, the administrative authority must request the judge of freedoms and detention to use the seized documents and data. If this request is denied, the copies are destroyed and the media returned.

With regard to intelligence, the law of 30 July 2021 amended Article L822-3 of the Internal Security Code. It allows a service that obtains information which is useful for a purpose different from that which justified its collection, to be able to transcribe or extract it for the sole purpose of carrying out its missions. These same services may transmit the information they have collected, extracted or transcribed to another service "if such transmission is strictly necessary for the performance of the tasks of the recipient service"[227].

The article does, however, make exchanges of intelligence subject to prior authorisation by the Prime Minister after consulting the National Commission for the Control of Intelligence Techniques (CNCTR) when the transmission of collected intelligence serves a purpose different from that for which it was collected. Transmissions of information collected, extracted or transcribed as a result of the use of an intelligence gathering technique that the recipient service could not have used for the purpose for which it was transmitted will also be subject to prior authorisation by the Prime Minister after consulting the CNCTR. These transmissions will have no effect on the retention period for each piece of information collected, which will run from the date it was collected. At the end of this period, each service will destroy the information, in accordance with the procedures defined by Article L822-4 of the Internal Security Code.

In Spain, the sole seizure of one of the devices referred to in the previous point, carried out during the search of the home, does not legitimise access to its contents, without prejudice to the fact that such access may subsequently be authorised by the competent judge.

In Norway, Searches are carried out under the same regime as in the French or Spanish Code of Criminal Procedure. In cases of flagrante delicto, it is not necessary to make a request to a judge. The search can be carried out by the judicial police officer. Outside this hypothesis, the search must be carried out with judicial authorisation. In the case of a seizure during a search, in principle, a police officer has to obtain the consent of the judicial authority in order to proceed[228]. However, a police officer may, by way of exception, decide to carry out a seizure without prior judicial authorisation in the sole event of an emergency. Indeed, it must be considered that the delay in carrying out the seizure would entail a risk (which is notably the case for flagrante delicto).

Besides, the Norwegian court may allow the police to read private information contained in the computer system on the basis of an order if the person is prosecuted for offences punishable by 10 years of imprisonment or more.

In the case of preventive measures, the Norwegian Code of Criminal Procedure allows a judge to authorise the police security service to seize data[229]. Article 17 of the Police Act of 4 August describes, among other things, the conditions for the use of coercive measures for preventive purposes. The court may, by order, authorise the police security service in the context of its

[226] Art. L.229-5 of the French Code de la sécurité intérieure.

[227] Art. L.822-3 of the French Code de la sécurité intérieure. [Online] Available: [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043887421/2021-07-31].

[228] Art 197 of the Norwegian Criminal Procedure Act. [Online] Available: [https://lovdata.no/dokument/NL/lov/1981-05-22-25/*#&].

[229] Norwegian Code of Criminal Procedure. [Online] Available: [https://lovdata.no/dokument/NL/lov/1995-08-04-53].

preventive activities to use certain measures of the Code of Criminal Procedure (including the one provided for in Art. 206, namely the reading of data, with the bypassing of the security of devices, by extension encryption)

In Germany, in the same way as in the above-mentioned countries, if there is a suspicion that an offence has been committed, the public prosecutor's office and the police can decide to carry out a search pursuant to Section 94 et seq. of the German Code of Criminal Procedure.

In principle, a warrant must be issued by a judge, but in urgent cases, the public prosecutor or the police can take the decision to search a home on their own. As regards data and objects, if they are of interest and considered as evidence, they can be seized after a judge has requested it by order.

As with the search, in urgent cases, the seizure may be carried out at the request of the public prosecutor or the police, but a judicial remedy will be available to the owner of the property seized.

In the Netherlands, as an exception, seizures under Article 94 of the Dutch Code of Criminal Procedure can be made without prior judicial review. The European Court of Human Rights has held that in a situation where an individual voluntarily gives his or her PIN code, and the police merely check a few messages in a targeted, non-secret search, the use of Article 94 is proportionate with respect to the right to privacy in that it does not allow for an overly severe invasion of privacy. that it does not allow for too severe an invasion of privacy.

However, the situation is different when the telephone is deciphered in the investigation by a forensic method. A 'search for the truth' based on Article 94 is too general and would leave too much discretion to the police. A simple ex post control is therefore not sufficient[230].

In the light of the right to privacy guaranteed by Article 8 of the European Convention on Human Rights, the Dutch Supreme Court has raised the importance of creating new regulations with effective safeguards for data seizures.

In the United Kingdom, in the context of data seizures, the Police and Criminal Evidence Act (1984) is the legislation that allows the police to seize and investigate digital devices to obtain evidence. For example, the police can obtain access to excluded material or material from a special procedure for the purposes of a criminal investigation if they request it.

Similarly, the police officer may require that any information that is stored in electronic format be accessible and produced in a way that can be taken away and that is visible and readable if he has reasonable grounds.

The Data Protection Act of 1998 provides that the processing of personal data is subject to eight principles of protection including that personal data should be processed fairly and lawfully and, most importantly that they are processed only if necessary for the administration of justice or the performance of any other public function carried out by any person in the public interest or if the processing of such data is sensitive and necessary for the purpose of or in connection with legal proceedings or for the administration of justice and is carried out in compliance with safeguards ensuring adequate protection of the rights and freedoms of data subjects.

In particular, Article 29 provides that the first principle, fairness, does not apply to personal data processed for the purpose of the prevention or detection of criminal offences except in so far as it requires compliance with the conditions set out in Annexes 2 and 3, i.e. for the administration of justice or where the processing is necessary for the purpose of legal proceedings. According to the fifth principle, personal data processed for a given purpose or purposes should not be kept for longer than is necessary to achieve that purpose or those purposes.

An Information Commissioner has an independent role in promoting compliance with good practice by data controllers and has the power to issue enforcement notices. The Act makes it an offence to

[230] The Dutch Supreme Court ruled in 2017 that this basis alone was insufficient for such a seizure because the existence of ex post control does not compensate for the absence of ex ante control for this type of infringement.

fail to comply with such directions and to obtain or disclose personal data or information contained therein without the consent of the data controller. Article 13 sets out the right to claim damages before the domestic courts for breaches of the Act's provisions.

In France and the United Kingdom, for example, a large number of intelligence services have been given prerogatives, which may pose a problem from the point of view of fundamental freedoms. It must be ensured that adequate safeguards are provided by the independent administrative authorities responsible for monitoring these measures. Indeed, the CNCTR (French supervisory authority) only has an advisory opinion on the technical measures implemented by the intelligence services, which would not be requested when an "emergency situation" is declared. This does not adequately ensure the respect for privacy guaranteed by the European Court of Human Rights, even though both countries are parties to the Convention. The United Kingdom also lacked transparency with regard to its mass interception techniques, which were only checked by the Prime Minister, which is why the United Kingdom was condemned in the ECHR judgment of 25 May 2021. Indeed, the European Court ruled that the UK government's powers of mass interception of communications "did not contain sufficient safeguards" throughout "to provide adequate and effective protection against arbitrariness and the risk of abuse", so that there was a violation of the rights to privacy and freedom of expression guaranteed by the European Convention on Human Rights.

Since the information collected and stored by the UK government can reveal the most intimate aspects of a person's private life, i.e. where they go, who they are in contact with, what websites they visit and when, etc., the UK government has a duty to protect its citizens. Finally, the Investigatory Powers Tribunal (IPT), the UK court responsible for investigating complaints against GCHQ, MI5 (counter-intelligence services) and MI6 (intelligence services), which had concluded that the practices used to collect this information and store it could comply with the UK's obligations in terms of privacy rights in particular, was contradicted by the Grand Chamber of the European Court. It is noteworthy that the Court has made it clear that states cannot delegate the power to authorise surveillance to the executive, nor can they treat hundreds of millions of citizens' private communications as an open-access commodity", said English legal adviser Kate Logan.

Similarly, on the issue of data retention, the European Court of Human Rights had already condemned the United Kingdom on 8 December 2008[231] with regard to the protection of privacy guaranteed by Article 8 of the European Convention on Human Rights. Two UK citizens had complained to the ECHR about the retention of their fingerprints, profiles and DNA samples in British police databases, even though they had been cleared or acquitted. They had previously been refused deletion of this data by the police authorities, as well as by all other levels of court, on the basis of the Police and Criminal Evidence Act 1984. The ECHR ruling was therefore a victory for privacy because the indefinite retention of fingerprints, cell samples and DNA profiles of unconvicted persons is recognised as a violation of Article 8 of the European Convention on Human Rights.

The ECHR is thus becoming increasingly attentive to data capture and protection.

4.7 Cooperation between investigative services

A principle of trust[232] exists between states on the propriety of the investigative methods used. Under this principle of trust, for example, a court will not assess privacy in the taking of evidence at trial[233]. Similarly, an investigative technique covered by national secrecy, such as the technique used by France in the Encrochat case, need not be submitted to the court in which the case is being tried.

[231] ECHR, S. and MARPER v. RU 8 décembre 2008. [Online] Available: [https://hudoc.echr.coe.int/eng#{"itemid":["001-90052"]}]

[232] The principle of mutual trust has its source in Article 2 TFEU.

[233] "Encrochat: juridisch kader onderzoekswensen", *Weening Strafrechtadvocaten, op. cit.* p. 11.

On the other hand, strong indications are necessary for a legality review to be carried out by the court. This indicates that in case of strong doubt, or in case of a presumed violation of a right protected by the ECHR, the judge should proceed to the legitimacy review[234].

4.7.1 Data exchange and cross-border investigation

4.7.1.1 The legal grounds

Alongside the Council of Europe's mutual legal assistance procedure and contact point established by the Budapest Convention, the European Investigation Order, established by Directive 2014/41/EU90[235], allows the cross-border exchange of information. This exchange concerns not only the content of telecommunications relevant to an ongoing criminal investigation, but also metadata[236], as a less intrusive alternative.

A further point of cooperation on information exchange between EU LEAs is provided for regarding metadata by Council Framework Decision 2006/960/JHA[237], and in the case of terrorism, cooperation simplifying the exchange of personal data is provided for by Council Decision 2008/615/JHA[238].

The report *Study on the retention of electronic communications non-content data for law enforcement purposes*[239] of September 2020 mentioned the lack of harmonised rules, the excessive length of time before obtaining the data, and the lack of knowledge of the practices of other Member States as the 3 major problems when requesting data.

This observation, apart from highlighting the need for better harmonisation of investigation procedures with a view to efficiency, also raises the more general issue of the modernisation of judicial systems. Numerous initiatives aimed at improving cooperation between investigation services and their digital tools have been planned for several years.

This modernisation includes a greater digitalisation of cross-border judicial cooperation[240], but also an improvement of the functioning of Eurojust and a greater implementation of their anti-terrorist register[241].

In the Big Brother Watch and Others v. United Kingdom case, the Court considers that the transmission of information obtained through mass interception to foreign states or international

---

[234] BRINKHOFF Sven, "Startinformatie in het strafproces", Deventer: Kluwer 2014, § 11.5.2.3.

[235] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, Official Journal L 130, 1.5.2014, pp. 1-36. [Online] Available: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041].

[236] *Ibid.,* cons. 30.

[237] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, Official Journal L 386, 29.12.2006, pp. 89-100. [Online] Available: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006F0960].

[238] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, Official Journal L 210, 6.8.2008, pp. 1-11. [Online] Available: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008D0615].

[239]European Commission, Directorate-General for Migration and Home Affairs, Dupont, C., Cilli, V., Omersa, E., et al., *Study on the retention of electronic communications non-content data for law enforcement purposes: final report*, Publications Office, 2020. [Online] Available: [https://data.europa.eu/doi/10.2837/384802].

[240] European Commission, « Modernising EU justice systems - Questions and Answers », 2 December 2020. [Online] Available: [https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2247].

[241] Riehle C., « 2019 Counter-Terrorism Report by Eurojust », 12 February 2021. [Online] Available: [https://eucrim.eu/news/2019-counter-terrorism-report-by-eurojust/].

organisations should be limited to material collected and retained in a manner consistent with the Convention, and that safeguards on the transfer must be put in place.

This means that domestic law must specify the **circumstances of such transfers**, that **the state must ensure that the receiving state has safeguards in place,** including safe storage and confidentiality, and that **stronger safeguards are needed for specifically protected data** such as confidential journalistic communications[242].

4.7.1.2 The need for technical modernisation of cross-border cooperation

The Proposal for a Regulation on a computerised communication system for cross-border civil and criminal proceedings (E-CODEX system)[243] aims to achieve this modernisation by generalising the use of the E-CODEX system in the Member States, thus helping to avoid legal fragmentation. The e-CODEX system, as a set of software components designed to connect national systems, thus allows the establishment of communication networks for cross-border cooperation, as well as the exchange of digital evidence and other related procedural media[244]. The Commission intends to entrust this system to the EU-LISA[245] agency as of 1 July 2023.

Another tool that should be more widely used by the services of the different Member States is the e-Evidence Digital Exchange System (eEDES), which also allows the exchange of European investigative decisions, mutual legal assistance requests and other evidence in digital format, within a secure architecture using two-factor authentication and encryption of the data sent.

There have been some warnings about the future framework of this cooperation. Indeed, the regulation providing for the generalisation of the use of these tools, which is still being evaluated, has recently been the subject of proposed amendments within the European Parliament on 15 October 2021[246]. These proposals show in particular that Annex I, containing a list of instruments providing for procedures subject to e-CODEX, should be deleted[247] in order to avoid any risk of overflowing the scope initially provided for by Article 2 of the Regulation, namely the exchange of data in the context of cross-border cooperation in civil and criminal matters. Among the proposed amendments, it is more generally considered that the proposed regulation allows for a step forward in the interoperability between national judicial systems[248].

---

[242] ECHR, 25 May 2021, Case of Big Brother Watch and Others v. United Kingdom, no. 58170/13, 62322/14 and 24960/15, §2. Big Brother Watch and Others v. the United Kingdom, nos. 58170/13, 62322/14 and 24960/15, § 362. [Online] Available: [https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2021/05/5817013.pdf].

[243] Proposal for a Regulation of the European Parliament and of the Council on a computerised system for communication in cross-border civil and criminal proceedings (e-CODEX system), and amending Regulation (EU) 2018/1726. [Online] Available: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0712].

[244] European Council, « Digitalisation of justice: Council presidency and European Parliament reach provisional agreement on e-CODEX », 8 December 2021. [Online] Available: [https://www.consilium.europa.eu/en/press/press-releases/2021/12/08/digitalisation-of-justice-council-presidency-and-european-parliament-reach-provisional-agreement-on-e-codex/].

[245] About EU-LISA, see: https://www.eulisa.europa.eu/

[246] European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on a computerised system for communication in cross-border civil and criminal proceedings (e-CODEX system), and amending Regulation (EU) 2018/1726 (COM(2020)0712 – C9-0389/2020 – 2020/0345(COD)), 15 October 2021. [Online] Available: [https://www.europarl.europa.eu/doceo/document/A-9-2021-0288_EN.pdf].

[247] *Ibid.*, p. 15.

[248] Ho-Dac M., « European Parliament Report on the Proposal for a Regulation on e-CODEX System », 19 October 2021. [Online] Available: [https://eapil.org/2021/10/19/european-parliament-report-on-the-proposal-for-a-regulation-on-e-codex-system/].

4.7.1.3 Future improvements in cooperation between law enforcement agencies and service providers

In more than half of all criminal investigations, a cross-border request is made to obtain electronic evidence held by service providers established in another Member State or even outside the European Union. However, the judicial cooperation and mutual legal assistance mechanisms that are necessary to obtain such data are extremely slow and burdensome[249]. According to the European Commission, "almost two thirds of crimes where electronic evidence is held in another country cannot be properly investigated or prosecuted, mainly due to the time it takes to gather such evidence or due to fragmentation of the legal framework".

Policy makers have recognised the need for LEAs to have access to certain information held by suppliers and other entities. The 2nd Additional Protocol to the Budapest Convention reinforces this direct cooperation[250] through two measures:

The identification of domain name holders (Art. 6). Although previously accessible to all using tools called WHOIS, certain information concerning the registration of a domain name is now restricted. This measure addresses this potential difficulty, while having the advantage of being less intrusive than other types of collection, as this information does not allow for precise conclusions to be drawn about an individual's private life[251].
Disclosure of subscriber data (Article 7). International cooperation procedures, such as mutual legal assistance, are not always the most effective tool for dealing quickly with the ever-increasing requests for electronic evidence[252]. This measure aims to simplify requests to service providers of other Parties to the Convention by allowing a prosecutor or other judicial authority to address the service provider directly in the form of an order to provide subscriber data.
The art 8 completes the cooperation between authorities: A Party may request another Party to order a service provider to expedite the production of subscriber and traffic data.

In addition to this, at EU level, the draft European e-evidence Regulation[253] would provide law enforcement authorities with better access to electronic evidence by putting in place "*unprecedented*

[249] Bismuth R., « Le Cloud Act face au projet européen e-evidence », *Revue critique de droit international privé*, 2019, p. 1.

[250] Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, as adopted by the Committee of Ministers on 17 November 2021, [Online], available: [https://rm.coe.int/1680a49dab].

[251] Council of Europe, Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, 17 November 2021, p. 14. [Online] Available: [https://rm.coe.int/1680a49c9d].

[252] *Ibid.* p. 19.

[253] 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),

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"[254].

Five main items are foreseen by this proposal to achieve its objective, notably through measures **targeting providers offering services in the EU and established or represented in another Member State**:

- **The European Production Order**: regardless of the location of the data, a judicial authority of a Member State will be able to request electronic evidence (such as emails, SMS or messages exchanged in applications) directly from a provider; the response time will be 10 days, or 6 hours in case of urgency (currently, the European Investigation Decision allows 120 days and the mutual legal assistance procedure 10 months).

- **The European Preservation Order**, to prevent the deletion of data: a judicial authority of a Member State will be able to compel a service provider to preserve certain data so that it can request this information at a later stage by mutual legal assistance, a European Investigation Order or a European Production Order;

- **The provision of strong safeguards and remedies**: injunctions will only be possible in criminal proceedings, with the procedural safeguards that this implies. Service providers and individuals whose data is requested will benefit from several safeguards, for example the request for a review if the service provider believes that there is a breach of the EU Charter of Fundamental Rights.

- The designation of a legal representative in the Union by service providers. In the same way as for the RGPD with the DPO, all service providers offering their services in the European Union will be subject to the same obligations, even if their headquarters are located in a third country. The receipt, compliance and enforcement of decisions and injunctions for the purpose of gathering evidence in criminal matters will be carried out by this representative;

- The improvement of legal certainty for service providers through identical rules for all, as well as for LEAs, which will no longer depend on the goodwill of service providers.

2018. [Online] Available: [https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN].

[254] European Commission, "Security Union: Commission facilitates access to electronic evidence". [Online] Available: [https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3343].

Chapter 5 Data protection

The protection of personal data plays a fundamental role in the exercise of the right to respect for private and family life enshrined in Article 8 of the European Convention on Human Rights, and it is therefore essential for the European Court that member states provide appropriate safeguards to prevent any use of personal data which is not in accordance with the safeguards laid down in Article 8.

In order to assess the lawfulness of the processing of personal data by LEAs, it is necessary to consider both the elements of the legal framework of criminal law that impose obligations on LEAs and the legislation on personal data protection in this respect.

As regards the use and processing of data in the context of criminal law, this subject has been explained in detail in the previous chapter of this document. Therefore, this part will only deal with data processing by LEA in the specific context of data protection legislation.

5.1 The EU legal framework on personal data protection

Regarding EU law, the GDPR and the Directive 2016/680 of 27 April 2016, known as "Law Enforcement Directive"[255], both make up the "European package on the protection of personal data". They have different but complementary scopes of application; the GDPR is intended to apply to all processing of personal data in the Member States, both in the public and private sectors, although it does not apply to processing carried out in the exercise of activities which do not fall within the scope of EU law, such as state security or national defence activities, and those carried out for the purposes of the Law Enforcement Directive (LED).

As for the processing of personal data in police and judicial files, the provisions applicable to these files are established by the law enforcement Directive.

For the processing of smartphone data seized by LEAs, the Law Enforcement Directive is therefore of paramount importance, with regard to the specific provisions on LEAs processing data for law enforcement purposes and especially with regard to cooperation between EU Member States, which requires each Member State to put in place measures to cooperate effectively[256].

5.1.1 Scope of the Law Enforcement Directive

As explained above, personal data obtained by LEAs have specific requirements and characteristics and the Law Enforcement Directive aims to address these, while including all the basic data protection principles set out in the GDPR.

This directive aims to strike a balance between the protection of personal data, and therefore the right of individuals to privacy, and the interest of LEAs; to improve cooperation in the fight against terrorism and cross-border crime in the EU by enabling police and criminal justice authorities in EU countries to exchange information needed for investigations more effectively.

However, there are two cumulative conditions for a processing operation to be considered within the scope of the law enforcement directive. Firstly, the processing must pursue one of the purposes specified in Article 1 of the Directive, which shows that the Directive is largely intended to apply to

[255] Directive n° 2016/680 of the 27 april 2016 (LED). [Online] Available: https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0680

[256] Article 50 of the LED.

"criminal matters" and, in particular, to activities carried out by police forces. According to its Article 1[257], the Police-Justice Directive establishes rules on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the protection against and prevention of threats to public security.

The provisions of the Directive may also be intended to govern processing operations carried out in the context of activities that relate to policing activities carried out prior to the commission of a criminal offence. Thus, the purposes covered may include preventive policing activities aimed at protecting against threats to public security which could give rise to a criminal charge (policing at demonstrations, sporting events, maintenance of public order, etc.) and the processing operations carried out for these purposes.

Secondly, the processing of personal data only falls within the scope of the law enforcement directive if it is carried out by a 'competent authority'. According to Article 7 of the Directive, this means

- any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (judicial authorities, the police, any other law enforcement authorities etc.); or,

- any other body or entity entrusted by the law of a Member State with the exercise of official authority and public prerogatives for the purpose of carrying out processing covered by this Directive.

Despite the seemingly broad approach of the law enforcement Directive, its actual scope is more limited than it appears at first sight. First of all, its scope is limited to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and does not cover the processing of personal data in the context of criminal judicial proceedings.

In other words, where personal data are processed in the context of criminal judicial proceedings, Member States may require that the exercise of the right to information, access and rectification or erasure of personal data be carried out in accordance with their national law[258].

In this respect, the real added value of the LED therefore depends on its implementation in national law and the willingness of national courts to ensure that the Directive is applied uniformly throughout the EU.

Furthermore, the Directive does not regulate the processing of personal data in the context of an activity that falls outside the scope of EU law[259]. This provision has been interpreted in paragraph 14 of the preamble[260] as covering activities concerning national security, activities of agencies or departments dealing with national security matters and the processing of personal data by Member States. However, until today, there is no uniform definition of these key concepts. Thus, until the European Court interprets it, the scope of the Directive again depends on how national courts will interpret the term 'activity falling outside the scope of Union law' and how Member States will decide to implement the Directive.

[257] Article 1 of the LED.

[258] Article 18 of the LED.

[259] Article 2, paragraph 3 of the LED.

[260] "Since this Directive should not apply to the processing of personal data in the course of an activity falling outside the scope of Union law, activities relating to national security, activities of agencies or departments responsible for national security matters and the processing of personal data by Member States in the course of activities falling within the scope of Chapter 2 of Title V of the Treaty on European Union should not be considered as activities falling within the scope of this Directive".

5.1.2 The principles of data protection with LED

5.1.2.1 Specific obligations of LEAs

The second chapter of the Directive sets out the general principles for the processing of personal data, with which the competent authorities must demonstrate compliance. Almost identical to the GDPR and incorporating most of the established data protection principles, the Directive stipulates that data processing activities must meet the requirements of purpose limitation, proportionality of data, accuracy, lawfulness, fairness, transparency and integrity and confidentiality:

➔ The principle of lawfulness, fairness and transparency of processing:

In order to be implemented, any data processing must be based on one of the 'lawful bases' provided for by the Directive. Article 8 of the Directive sets out the grounds for lawfulness: the processing must be necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the protection against and prevention of threats to public security (i.e. the purposes set out in Article 1(1)), by the competent authorities. Furthermore, the processing must be based on Union law or the law of a Member State.

Compliance with the fairness principle mainly requires that the data subjects of the processing operation be informed prior to the collection of personal data. Individuals should be informed of the risks, rules, safeguards and rights with regard to the processing of their personal data and how to exercise their rights in relation to the processing. Therefore, when a telephone is taken into possession by LEA, officers should provide detailed information to the person from whom the device is taken or acquired, containing:

- the facts about what is being sought from the device
- on what legal basis; and
- the rights of the individual in relation to that processing (from Article 13 to Article 17 of the Directive).

This does not in itself prevent law enforcement authorities from carrying out activities such as covert investigations or video surveillance[261]. Such activities may be carried out for the purposes set out in Article 1(1) of the Directive, provided that they are determined by law and that they constitute a necessary and proportionate measure in a democratic society, having due regard to the legitimate interests of the individual concerned.

➔ The principle of purpose:

Processing must be limited to a purpose determined at the time of collection of personal data and must also be explicit and legitimate and must not be processed in a way incompatible with the purpose for which it was collected.

➔ The principle of proportionality and relevance:

The data processed must be relevant and strictly necessary for the purpose of the file. In other words, the personal data collected must not be excessive in relation to its purpose.

➔ The principle of accuracy:

Data must be accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data which are inaccurate, having regard to the law enforcement purpose of their processing, are erased or rectified without delay.

[261] Recital no. 26 of the LED.

➔ The principle of limited retention:

Personal data collected shall not be kept for longer than is necessary for the purposes for which they are processed.

➔ The principle of security and confidentiality:

Adequate measures must be put in place to ensure appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

However, it is important to note that all the practical guidelines of Council of Europe Convention No. 108[262] and Recommendation R (87) 15 have not been followed, since the data minimisation clause only requires that the collection of data is 'not excessive' rather than 'limited to the minimum necessary' and a number of additional safeguards have been omitted. For example, the Convention 108 states that further use for different purposes should only be allowed if it is provided for by law, necessary in a democratic society, precise, foreseeable and proportionate to the aims pursued. Moreover, the lack of concrete criteria for a periodic review of the need for storage of personal data and the mere requirement of 'appropriate' time limits rather than a precise timetable are regrettable in the light of the recent case law of the Court of Justice of the European Union (CJEU).

On the other hand, there are other obligations specific to the Directive, which are incumbent on LEAs. Namely:

➔ Article 6 of the Directive requires LEAs to make, where appropriate and possible, a clear distinction between the data of different categories of data subjects. In doing so, the Directive recognises the importance of classifying and processing data differently depending on the degree of involvement of the data subject in a crime. As such, a distinction should be made between: (a) persons suspected of having committed a crime provided that there are serious grounds or persons who are about to commit a criminal offence, (b) persons convicted of a criminal offence, (c) potential victims and certain victims of a crime and (d) other parties such as witnesses, contacts and informants.
As to these distinctions introduced by the Directive, the fact that they only have to be respected 'as much as possible', as well as the lack of specific safeguards for non-suspects or different types of crime and the lack of technical and organisational criteria make it difficult to comply with these provisions in a practical and uniform way.

For example, the European Data Protection Board (EDPB) recommended that the processing of personal data of non-suspects "should only be allowed under certain specific conditions and when absolutely necessary for a legitimate, well-defined and specific purpose" and that additional safeguards should be implemented[263].

➔ LEAs should, as far as possible, check the quality of personal data; they should distinguish between data based on facts and data based on personal judgements[264].

[262] The Council of Europe, *Convention No. 108 on the protection of data with regard to automatic processing of personal data*, *op. cit*.

[263] Article 29 Data Protection Working Party, "Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive", 26 February 2013, p. 3.

[264] Article 7 of the LED.

- ➔ There are additional protections for sensitive data[265]. Processing of sensitive data is defined as processing:
  - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
  - genetic data, biometric data for the purpose of uniquely identifying a natural person;
  - data concerning health, and
  - data concerning the sexual life or sexual orientation of a natural person.

  The processing of such sensitive data is permitted only where absolutely necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:

  - when authorised by Union law or the law of a Member State
  - to protect the vital interests of the data subject or of another natural person; or
  - when the processing relates to data which are manifestly made public by the data subject.

5.1.2.2 Rights of the data subject

Due to the specificity of the scope of the Law Enforcement Directive, some rights contained in the GDPR are not found in the Directive (e.g. the right to data portability) or may be subject to limitations.

The general modalities for exercising these rights are set out in Article 12 by requiring that requests from data subjects are followed up without undue delay and that information is made available in a concise, intelligible, generally free and easily accessible form. The rights of data subjects recognised in the Directive are as follows:

- ➔ information of the data subject, subject to possible limitations (Article 13). In this respect, the Directive requires the controller to make available to the data subject at least the following information

  (a) the identity and contact details of the controller;

  (b) where appropriate, the contact details of the data protection officer

  (c) the purposes of the processing operation for which the personal data are intended

  (d) the right to lodge a complaint with a supervisory authority and the contact details of that authority

  (e) the existence of the right to request from the controller access to, rectification or erasure of personal data and the restriction of the processing of personal data relating to a data subject

  In addition to the information mentioned above, the second paragraph of Article 13 of the Directive requires Member States to provide by national law that the data controller shall, in specific cases, provide the data subject with additional information to enable him to exercise his rights. The mentioned information is:

  (a) the legal basis for the processing,

  (b) the period for which the personal data are to be kept or, where this is not possible, the criteria used to determine that period

  (c) where appropriate, the categories of recipients of personal data, including in third countries or within international organisations

[265] Article 10 of the LED.

(d) where necessary, additional information, in particular where personal data are collected without the knowledge of the data subject.

However, the Directive not only does not explain these "special cases" but also allows Member States to adopt legislative measures to delay or restrict the provision of the information specified in paragraph 2, or not to provide such information, where and for as long as such a measure constitutes a necessary and proportionate step in a democratic society, having due regard to the fundamental rights and legitimate interests of the data subject in order to:

(a) avoid obstructing official or judicial enquiries, investigations or proceedings,

(b) avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,

(c) protect public security,

(d) protect national security or

(e) protect the rights and freedoms of others.

- ➔ the right of access (Article 14), subject to limitations, in whole or in part, that may be imposed, in particular to avoid hindering investigations, preventing and detecting criminal offences, etc. (Article 15). In practice, the limitation of the right of access may result in the implementation of an "indirect right of access", i.e. exercised through the competent supervisory authority (Article 17). For example, certain files, such as police files and files concerning State security, are particularly restricted and access to these files is indirectly granted through the supervisory authority.

- ➔ the right to rectification or erasure of personal data (Article 16). The Directive gives data subjects the possibility to obtain the rectification or erasure of their personal data and, in certain cases, the restriction of their processing, as soon as possible. Their personal data can be rectified when inaccurate and erased in case of legal obligation or breach of certain data protection standards.

However, in the event that a data subject's rights to obtain information, access and rectification or erasure of personal data are restricted or refused by reason of the exceptions mentioned above, Article 17 gives the data subject the possibility to instruct the supervisory authority to exercise these rights on his or her behalf. Although this does not constitute an indirect method for the data subject to obtain the desired information, access or erasure, the supervisory authority must carry out all necessary checks and examinations of the data processing and inform the data subject of the outcome of these checks and examinations.

5.1.3 Transfers of personal data to a third country

Article 40 rules to promote cooperation in protecting personal data

In relation to third countries and international organisations, the Commission and Member States shall take appropriate steps to:

- ➔ Protect personal data through cooperation mechanisms
- ➔ Mutual assistance actions including notification, complaint referral, investigative assistance and information exchange shall take place under appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;
- ➔ Engage in discussions with key stakeholders for better international cooperation for data protection
- ➔ promote the exchange and documentation of practices and legislation

The Directive aims at harmonising the protection of personal data and thereby supporting the possibility of cooperation of law enforcement authorities through the exchange of such data. There is also a need for bilateral and multilateral cooperation of national supervisory authorities. This need is amplified by the trend towards constant cross-border interconnection of databases, the interoperability regulations being only one of many projects in this respect. As provided for in Chapter VII of the Directive, the EDPB stresses the need for close cooperation between Member States[266].

In order to provide a framework for such cooperation, a number of general principles are laid down in Article 35. The transfer of personal data to third countries must be necessary for the purposes of the processing provided for by the Directive and may only take place when the conditions described below are met. The controllers transmitting and receiving the data must be competent authorities, and the Member States transferring the data must authorise onward transfers to other third countries or organisations after considering the relevant factors.

If data from another Member State is transferred, the Member State from which the data originate must authorise the transfer, unless it is necessary for the prevention of an immediate or serious threat to public security. In addition, Article 40 sets out a number of ground rules to promote international cooperation and facilitate the exchange of information by identifying appropriate steps towards a more inclusive and comprehensive data protection framework for international exchanges.

Article 36 describes the first situation in which data can be transferred to a third country, namely when the European Commission has issued an adequacy decision establishing that this nation offers sufficient guarantees for the protection of European personal data. In the absence of such an

[266] Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62, adopted on 14 December 2021.

adequacy decision, Article 37 provides that it is the responsibility of the transferring country to ensure that adequate standards of data protection exist in the receiving country, either by confirming that a legally binding instrument provides appropriate safeguards, or by assessing all the relevant circumstances surrounding the transfer and concluding that such safeguards are indeed present.

As suggested in recital 71 of the Directive, this assessment could include cooperation agreements between Europol or Eurojust and third countries, confidentiality obligations, the implementation of the specificity principle and whether the data could be used to support any form of cruel and inhuman treatment.

In the absence of an adequacy decision or appropriate safeguards, Article 38 states that data may only be transferred to third countries if this is necessary to protect the vital interests of a person, to safeguard the data subject's legitimate interests or to prevent immediate and serious threats to public security.

This legal framework of procedures and rules for data exchanges with third countries marks a step forward in international cooperation of law enforcement and judicial authorities. However, as is the case with other provisions of the Directive as explained above, the vague provisions on the establishment of appropriate safeguards by the transferring country allow Member States to implement and use divergent adequacy standards. Such a lack of uniform standards and protocols could lead to divergent national implementations and transfers to countries with lower data protection standards than originally envisaged.

Similar concerns may be raised about the transfer of data in the absence of adequacy decisions or appropriate safeguards. Due to the vague wording and broad scope, these conditions may also lead to divergent interpretations by Member States.

5.1.4 The challenges of transposing the LED

The Law Enforcement Directive establishes a minimum harmonisation, leaving Member States the possibility to adopt higher standards than those laid down in the Directive and to provide additional safeguards for the protection of personal data, which leaves a wide margin of discretion to Member States.

Nevertheless, this choice creates challenges regarding the harmonisation and coherence of the protection of personal data in the EU, especially when one considers the choice of wording of the key concepts of the directive. Some of the provisions of the Directive are formulated in a very general way, because, according to the EDPB, they are the result of a compromise between different interests and political perspectives[267]. Therefore, some of the legal provisions of the Directive may be subject to different interpretations, such as the scope of the Directive, explained above, and the powers of the competent authorities.

For example, in France, the directive was transposed by Law No. 2018-493 of 20 June 2018[268] on the protection of personal data, one and a half months after the transposition deadline.

France had the advantage in this area of having a Data Protection Act (*Loi Informatique et Libertés,* LIL) which had already applied to files in the government sector since 1978 and the transposition of Directive 95/46 EC, which did not cover these issues. In this respect, the transposition of the directive did not lead to a radical change in the French legislative framework. However, this was not the case

[267] Contribution of the EDPB to the European Commission's evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62, adopted on 14 December 2021.

[268] Loi n°2018/493 relative à la protection des données personnelles, *JORF 21 June 2018*. [Online] Available: [https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952].

in other States, particularly those that had no legislation in this area prior to the directive. The Law Enforcement Directive was therefore a great novelty for them.

As previously explained, the transposition of the Directive also applies to national processing, which has an impact on national police and judicial files such as judicial records files or genetic and fingerprint databases.

As for the transposition of the provisions of the Directive in France, the same formula of the Directive, which was not clear on the definition of the scope of application having vague formulations, was used in the article of 86 of the LIL. The LIL speaks of "purposes" that will be carried out by certain "competent authorities" but the terms used in this article do not clearly specify the processing operations covered by the Directive.

One of the critical points of the LED was the vague terminology used, which leaves a very wide discretion to the Member States, which jeopardises the harmonisation of the Directive in the EU, and similarly, the lack of precision is also the case with the transposition of this Directive in France. In this respect, the lack of clarification of the concepts and criteria for identifying which types of processing fall within the scope in French law leaves a wide discretion to LEAs. For example, in practice, the distinction between criminal and administrative authorities is not always clear. Similarly, in some cases, the distinction between the notion of criminal offence and administrative sanction is difficult for LEAs to make.

This lack of precision leads to confusion between the application of the RGPD and the Law Enforcement Directive. The choice to be made between the two will change the obligations of the controller and the rights granted to data subjects.

Another point that may give rise to confusion concerns hybrid files, which by virtue of their purpose are simultaneously covered by the Directive and other purposes under national law. This is the case with purposes relating to national security. On this point, the French Conseil d'État proposes to align the rights of data subjects at least with those of the directive.

"*In the case of processing operations falling within the scope of both the Directive and national law, where the data on which the data subject requests to exercise his or her rights cannot be linked exclusively to either of these two fields, the restrictions placed on these rights may not exceed those provided for by the Directive*"[269]

Apart from these broad delimitation rules, the transposition could be criticised for not clearly identifying the national processing operations that fall within the scope of Title III of the transposition law, i.e. the provisions applicable to processing operations falling under the Directive. Moreover, no document provides an exhaustive list of national processing operations, which makes it even more difficult for LEAs to decide on the applicable provisions. This transparency problem needs to be addressed.

Similarly, the uncertainty as to whether or not processing operations relating to "public security" fall within the scope of the provisions of the LIL, transposed from the Law Enforcement Directive, is another issue that creates legal uncertainty that can be detrimental to data controllers, in a context where police files are regularly challenged for their non-compliance.

More importantly, the transposition of the Directive into national law, which required the amendment of numerous pieces of legislation, has been subject to delays in several Member States. On 5 May 2016, the Directive entered into force. According to Article 63(1) of the Directive, Member States had

[269] "In the case of processing operations falling within the scope of both the Directive and national law, where the data on which the data subject requests to exercise his or her rights cannot be linked exclusively to either of these two fields, the restrictions placed on these rights may not exceed those provided for by the Directive.", French Conseil d'État. [Online] Available: *[https://www.conseil-etat.fr/ressources/avis-aux-pouvoirs-publics/derniers-avis-publies/adaptation-au-droit-de-l-union-europeenne-de-la-loi-n-78-17-du-6-janvier-1978-relative-a-l-informatique-aux-fichiers-et-aux-libertes].*

to adopt and publish the laws, regulations and administrative provisions necessary to comply with the Directive by 6 May 2018. More than three years later, this transposition has not been fully achieved in all Member States.

This was the case with Spain, for example: on 25 February 2021, the CJEU ordered Spain to pay a penalty of €15 million and a daily penalty payment of €89,000 for its persistent failure to transpose the Law Enforcement Directive before the deadline for transposing the rules of the Directive into national law, which ended on 6 May 2018[270]. As Spain did not provide any information on the transposition measures, the European Commission initiated infringement proceedings in July 2018 and referred the case to the CJEU on 25 July 2019.

In the proceedings before the CJEU, Spain did not contest the failure to transpose, but pointed to the exceptional political and institutional circumstances that prevented the country from adopting the necessary organic law to transpose the Directive and which should be taken into account for the proportionality of the penalties. The CJEU found that the imposition of a lump sum and penalty payment is justified in this case since Spain has persisted in its failure to fulfil its obligations[271].

As a result of this judgment, Law no. 7/2021, of 26 May, on the protection of personal data processed for the purposes of the prevention, investigation, detection and prosecution of criminal offences and the execution of criminal penalties, transposing the Law Enforcement Directive, was published on 27 May 2021 in the Spanish Official Bulletin[272].

On 25 June 2019, the European Commission also initiated proceedings against Germany for not having fully transposed the Directive. The Commission noted that only 10 of the 16 German states (Länder) had adopted transposition measures by the end of the transposition period on 6 May 2018[273].

As the European Commission has made clear, the failure to transpose the Directive not only leads to problems in the exchange of law enforcement information, but also to unequal treatment of individuals with regard to the protection of their fundamental rights. This will also be the case if Member States transpose these provisions in very different ways, due to the lack of precision regarding the concepts and the minimum level of harmonisation provided for by the Directive, as explained above.

5.2 Police and judicial files

Police files, for which there is still no unified definition, are a perfect example of the balancing of general and private interests in the defence of the fundamental rights and freedoms of individuals. Facilitating the resolution of investigations, the prevention of offences and cooperation between European and international police offices, the legitimacy of police files is nevertheless questioned. Based on criteria left to the discretion of the authorities that feed them, there are risks to the fundamental rights and freedoms of the people whose data are processed. In addition to the right to protection of their personal data, the rights to privacy and to the presumption of innocence may also be affected. Safeguards must therefore accompany the establishment of such files in order to guarantee the legal security of the persons concerned and to prevent mass surveillance, all the more so in the context of international cooperation.

---

[270] CJUE, press release No. 22/21 of the 25 february 2021. [Online] Available: [https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-02/cp210022fr.pdf].

[271] *Ibid*.

[272] Highlights of the Spanish Act on Data Protection in the Area of Police and Criminal Justice (Organic Law 7/2021), QUEZADA Katherine, 15 juin 2021. [Online] Available: [https://www.law.kuleuven.be/citip/blog/highlights-of-the-spanish-act-on-data-protection-in-the-area-of-police-and-criminal-justice/].

[273] Wahl T., *Infringement Proceedings for Not Having Transposed EU Data Protection Directive*, 10 September 2018. [Online] Available: [https://eucrim.eu/news/infringement-proceedings-not-having-transposed-eu-data-protection-directive/].

5.2.1 National police files: the case of France

In France, police files are specific administrative files whose purpose is to maintain public order. While their usefulness for prevention purposes is established, police files are on the verge of being tools of repression, the contours of which must be traced and safeguards imposed in order to avoid drifting into mass surveillance. Chapter II of Title IV of Book I of the French Code of Criminal Procedure deals with the issue of police files (Articles 230-1 to 230-46). It distinguishes between three types of file: background files, serial analysis files and the file of wanted persons. It is in these texts, apart from those dedicated to specific files, that the limits of police files are set.

French police files can only be used by law enforcement agencies within a strictly established framework. Indeed, the Loi Informatique et Liberté, reinforced by the Law Enforcement Directive, imposes a priori control of these files by the CNIL, the competent authority for the protection of personal data, pursuant to its Article 31: " I. – […] The processing of personal data implemented on behalf of the State and:

1° Which concern State security, defence or public safety; 2° Or which have as their object the prevention, investigation, recording or prosecution of criminal offences or the execution of criminal sentences or security measures. The opinion of the commission is published with the order authorising the processing."

The law imposes stricter control in the event that sensitive data is processed in the context of a police file by requiring a decree issued by the Council of State to authorise implementation after a reasoned and detailed opinion from the CNIL[274].

A posteriori, the CNIL has its usual powers of control, namely those allowed to regulatory authorities by the Law Enforcement Directive in Article 47 (investigations, examinations, sanctions, etc.) on its own initiative or on the basis of alerts. To further protect individuals who become aware of irregularities in the processing of personal data, the Directive requires competent authorities to put in place "effective mechanisms to encourage the confidential reporting of breaches of this Directive" in Article 48. Out of 29 checks carried out by the CNIL between 2015 and 2018 on processing operations carried out by the Directorate General of the National Police, the Directorate General of the National Gendarmerie and the Paris Police Prefecture, only two formal notices were issued but no sanctions were imposed.

In the context of police files, certain processing operations are automatically excluded in order to provide the best possible protection for the individuals whose data are processed. For example, interconnection is defined by the CNIL as "the linking of at least two files or personal data processing operations within the framework of an automated process whose purpose is to link information from these files or processing operations"[275]. Interconnection, which differs from matching in that it is automatic, presents risks in that it makes it possible to deduce information that gives rise to new data processing based on the latter. To avoid abuses, the interconnection of police files is subject to the opinion of the CNIL prior to ministerial or the French Conseil d'Etat authorisation[276]. Interconnection is prohibited in the case of certain files containing sensitive data, the result of which could be harmful to the persons concerned. No interconnection is possible between the automated national criminal record and any other national file or processing of personal data, which avoids the risk of disclosure of a person's criminal record.

Finally, depending on the file concerned, the protection of individuals is more or less reinforced according to the sensitivity of the data. We will take the case of the three most problematic files because of the sensitive data they contain.

---

[274] Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*, Article 31.

[275] CNIL, « Comment déterminer la notion d'interconnexion ? » [online], available: https://www.cnil.fr/en/node/15316 [consulté le 06/01/2021].

[276] Loi n° 78-17 du 6 janvier 1978 *relative à l'informatique, aux fichiers et aux libertés*, Article 33 3°.

5.2.1.1 The Criminal records processing file *Traitement des antécédents judiciaires (TAJ)*

The TAJ is a file shared between the police and the national gendarmerie which is used for judicial investigations in the search for the perpetrators of offences, but also in the case of administrative investigations, for example in the case of a preliminary investigation prior to the granting of a sensitive employment[277]. Identification data of defendants and victims of crime are recorded in this file, including the identity photo, which can be used for facial recognition. Sensitive data may also be included in this file, such as data resulting from the nature or circumstances of the offence or data relating to particular physical features, objects and permanence, as a means of identifying the person.

Safeguards are in place to protect the data in this file. Access to the file is limited to duly authorised persons only, i.e. national police and gendarmerie officers and military personnel carrying out individually designated judicial police missions, judicial customs officers, public prosecutors and judicial services officers authorised by the Public Prosecutor for judicial investigations, and authorised police and gendarmerie personnel, officers of the specialised intelligence services mentioned in Article R. 234-2 of the Internal Security Code, agents of the National Service for Administrative Security Investigations (SNEAS) and the Specialised Command for Nuclear Security (CoSSeN), as well as staff with administrative police responsibilities authorised by the State representative in the context of administrative investigations. Retention periods are established according to the age of the person concerned (20 years for adults and 5 years for minors) but exemptions exist according to the seriousness of the offence committed. As regards victims, their data is kept for a maximum of 15 years.

Besides, Article 230-8 of the Code of Criminal Procedure relating to the possibilities of obtaining the deletion of recorded personal data was the subject of a priority question of constitutionality (QPC) before the French Conseil Constitutionnel, whose decision of 27 October 2017 was to censure the provisions of the article deemed too restrictive and therefore infringing on the privacy of the persons concerned. Only those who were acquitted or had their case dismissed could have their data erased from the TAJ in advance, leaving those who were found guilty but exempt from penalty[278].

The Conseil d'État also accepted the legality of the TAJ, considering in its decision No. 360759 of 11 April 2014 that the file did not excessively infringe the presumption of innocence or respect for private life because sufficient legal and regulatory guarantees had been put in place[279].

The Ministry of the Interior, which is the data controller, is obliged to make the necessary efforts to provide information to the persons concerned by the processing of their personal data in the context of the TAJ. Nevertheless, the right to object is not possible to exercise, except for victims whose perpetrator has been definitively convicted[280].

This file is authorised to be interconnected with other files and data processing systems, namely the police and gendarmerie procedure drafting system (LRPPN and LRPGN), the customs procedure drafting software (LRPDJ) and the CASSIOPEE data processing system, in order to feed the file[281].

[277] Art. 230-6 to 230-11 of the French Code of Criminal Procedure.

[278] French Constitutional Court, decision no. 2017-670 QPC of 27 October 2017. [Online] Available: https://www.conseil-constitutionnel.fr/decision/2017/2017670QPC.htm

[279] French Conseil d'État, decision no. 360759 of 11 April 2014, *Ligue des droits de l'homme : AJDA 2014,* p. 823.

[280] Art. R. 40-33, I of the French Code de procédure pénale.

[281] CNIL, deliberation no. 2011-204 of 7 july 2011. [Online] Available : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000025804888

5.2.1.2 The French National DNA database *fichier national automatisé des empreintes génétiques (Fnaeg)*

The Fnaeg is a file established under the responsibility of the central directorate of the judicial police at the Ministry of the Interior. Under the control of a magistrate, it aims to facilitate the identification and search for perpetrators of offences using their genetic profile, as well as for missing persons using the genetic profile of their descendants or ascendants[282]. Articles 706-54 to 706-56-1-1 of the Code of Criminal Procedure define the legal framework for this police file. According to the CNIL, the file centralises the genetic data of unidentified persons (fingerprints from samples taken at the scene of an offence) and identified persons (persons convicted or implicated for one of the offences listed in Article 706-55 of the Code of Criminal Procedure). Article 706-55 lists the offences for which a DNA sample may be requested (sexual offences, offences against the person, drug trafficking, theft, extortion, fraud, serious destruction or damage, receiving stolen goods, terrorism, criminal association, etc.). When available, the following data are also entered into the file: surname, first names, date and place of birth, parentage and sex; the service that reported the case; the date and place where the report was drawn up; the nature of the case and the procedure reference.

Guarantees are provided for the maintenance of this file due to the extreme sensitivity of the data contained therein. First of all, the context of the processing is limited to the investigation of a crime or offence, a preliminary investigation, a rogatory commission or the execution of a search order issued by a judicial authority. The retention periods are defined, even if very long (between 25 and 40 years), and access to the file is limited. Indeed, only authorised staff of the sub-directorate of technical and scientific police of the central directorate of the judicial police, the national police and the national gendarmerie, persons assigned to the central service for the preservation of biological samples and specially authorised agents of international cooperation bodies in the field of judicial police or of the police or judicial services of foreign states under the conditions laid down in Article R.53-19-1 of the code of criminal procedure may consult the data.

Since 2010, the Constitutional Council has considered that the legislative framework relating to the FNAEG complies with the Constitution, provided that the length of time personal data is kept is proportionate to the seriousness of the offences concerned[283]. The ECHR does not seem to share the opinion of the Constitutional Council and takes its opposite view by condemning France for violating Article 8 of the Convention because of the excessive length of time genetic data is kept and the impossibility of obtaining its deletion, the latter infringing the fundamental right to private life[284].

5.2.1.3 The automated fingerprints database *fichier automatisé des empreintes digitales (FAED)*

The FAED is a file that centralises fingerprints and palm prints for the purpose of identifying the perpetrators of crimes and offences, searching for missing persons, identifying dead or seriously injured persons, as well as verifying the identity of a person stopped in the context of an identity or residence permit check[285].

In addition to fingerprints, the FAED shall contain the gender of the person and, where known, his/her surname, first name(s), date and place of birth and parentage, the nature of the case and the

[282] Legal and administrative information directorate, "Automated National DNA File (Fnaeg)", [Online] Available: [https://www.service-public.fr/particuliers/vosdroits/F34834]. [Accessed 12 janvier 2022]

[283] French Constitutional Court, decision no. 2010-25 QPC of 16 September 2010. [Online] Available: https://www.conseil-constitutionnel.fr/decision/2010/201025QPC.htm

[284] ECHR, 22 June 2017, no. 8806/12, *Aycaguer v. France*, [Online] Available: [https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-174441%22]}].

[285] Legal and administrative information directorate, "Automated Fingerprint File (Faed)", [Online] Available: [https://www.service-public.fr/particuliers/vosdroits/F34835]. [Accessed 12 janvier 2022]

reference of the procedure; the service which reported or recorded the traces; the date and place where the record was drawn up and, where applicable, the place and date of the trace collection; the origin of the information and the date it was recorded in the processing system, for fingerprints and palm prints transmitted in the case provided for in Article 3(5) of Decree No 87-249 and for print traces.

The persons whose data may be recorded in the file are listed exhaustively. These are suspects and fingerprints found on corpses. Persons sentenced to a custodial sentence may also have their fingerprints recorded in the file. If the identity of a deceased person cannot be established, his or her fingerprints may also be included in the file.

This file is also subject to a very strict framework in terms of personal data protection, which is all the more reinforced given the sensitivity of the data contained in it. The retention period of the data available in the file varies between 10 and 25 years depending on the seriousness of the offence and the status of the persons concerned since the decree n° 2015-1580 of 2 December 2015. Access to the file is limited to duly authorised civil servants and military personnel from the national police's criminal identification services, the national gendarmerie's central criminal intelligence service, and the national gendarmerie's research units.

The persons concerned by the processing of their data have the possibility of exercising their rights, in particular of access, rectification and deletion, with the data controller by contacting the Service Central de la Police Technique et Scientifique. For deletion, the request must be accompanied by a request to the public prosecutor and a protest in the event of refusal is possible before the judge of freedoms and detention.

As a symbol of the control and importance given to the protection of these sensitive files, on 24 September 2021, the CNIL's restricted formation sanctioned the Ministry of the Interior for its poor management of the automated fingerprint file (FAED), publicly reminding it of the need to comply with the legislation in force on the protection of personal data[286]. The CNIL noted the existence of data in the file that was not initially foreseen, an excessive duration in relation to the purpose of the processing, the lack of security measures and the absence of information to the persons concerned. These shortcomings were sanctioned by an injunction to comply before 31 October 2021, i.e. one month after the decision was handed down.

Despite attempts to protect data within states, and even considering the increasing need for cross-border investigations, international cooperation has the effect to undermine the rights of individuals because, in addition to opening up access to data to a larger number of people, data are pooled in databases that encourage the risk of interconnection.

5.2.2 At the international level

Although personal data are processed within the framework of international or community police cooperation organisations, the fact remains that, to date, there is no police file that is not a shared compilation of data initially from national police files. In any case, these centralised files are not exempt from the need to guarantee the fundamental rights of individuals.

5.2.2.1 Interpol

Internationally, Interpol is the largest police cooperation organisation, bringing together more than 190 states. Within this framework, a considerable amount of data is processed, often of a personal nature, "thanks to a centralised, structured and secure information and communication system whose purpose is to collect, process and disseminate information useful to the world's police forces, with the files constituting the main tools"[287]. Data from national police files may therefore be found

[286] CNIL, deliberation no. SAN-2021-016 of 24 September 2021. [Online] Available : https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044115170

[287] FRAYSSINET (J.), « Interpol et ses fichiers », 2017, p.3.

on the Interpol information system to form databases common to the various Interpol member countries. One of the guarantees provided by Interpol is that each country can choose which data to share with its foreign counterparts. This guarantee is coupled with the fact that countries can also determine which countries and authorities have access rights to the data. The data is thus well partitioned by country and access rights are limited to authorities deemed legitimate by the country issuing the data[288].

In addition, in order to protect the fundamental rights of individuals, Interpol is subject to specific data protection regulations. In the absence of an internationally binding text on data protection, Interpol, as an international organization, has chosen to submit to its own data processing rules[289]. These include the main principles relating to the processing of information similar to those of the GDPR and the Law Enforcement Directive. This regulation also makes it possible to establish the scope of relations between international and private entities, subjecting the sharing of data to very strict conditions, such as the approval of the relationship by the General Assembly of the General Secretariat and the respect of the principle of data minimisation, as well as the limitation of access[290].

In order to ensure that personal data is protected, an independent authority, the Commission for the Control of Interpol's Files (CCF), monitors the processing of personal data relating to the Organisation's activities and deals with complaints from people wishing to exercise their rights in relation to their data[291]. However, as its powers are limited to Interpol, the CCF does not replace the national supervisory authorities, which remain competent in the event of an investigation or sanction.

5.2.2.2 Europol

The European Union Agency for Law Enforcement Cooperation, Europol, is also, for the same reasons as its counterpart Interpol, required to process a lot of personal data in the course of its work. In the course of its activities, Europol operates an extensive data processing system.

The EIS, the Europol Information System, is a database which centralises the criminal data available within the organisation on serious international crimes, on suspected or convicted persons, on criminal organisations and offences and on the means used to commit them. This data is stored in the Europol IS and is partitioned there according to the type of data. However, it is possible to link this data in order to restore a specific criminal case for example. The feeding of the EIS must comply with traditional data protection principles and access to the data is limited to employees of the Agency, Member States' liaison officers, national experts seconded to Europol headquarters as well as persons working in Europol National Units and in the competent national authorities. In addition, external persons, such as partners, may consult through the Europol Operational Centre. Designated authorities of the Member States have the right to search the system.

In order to ensure the compliance of Europol's processing of personal data, the EDPS, the European Data Protection Supervisor, has representative units within the Agency[292].

---

[288] *Ibid.*

[289] INTERPOL, « Règlement d'INTERPOL sur le traitement des données », [III/IRPD/GA/2011 (2019)], [Online] Available: https://www.interpol.int/content/download/5694/file/24%20F%20RPD%20UPDATE%207%2011%2019_ok.pdf?inLanguage=fre-FR

[290] Articles 27 and 28 of the INTERPOL's Rules on the Processing of Data.

[291] Commission for the control of INTERPOL's files (CCF), [Online] Available: https://www.interpol.int/fr/Qui-nous-sommes/Commission-de-controle-des-fichiers-d-INTERPOL-CCF

[292] EUROPEAN PARLIAMENT AND COUNCIL, Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, 11 May 2016, JOUE L 135 of 24 May 2016, p. 53–114.
[Online] Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0794

5.2.3 The Schengen Information System

The SIS II file, which stands for Schengen Information System II, is a European police file whose guarantees for individuals are legally established, even if certain prerogatives remain at the discretion of the competent authorities. In this file, persons wanted for arrest or extradition or in the context of criminal proceedings, missing persons, certain persons banned from entering the country or objects wanted for seizure or in the context of criminal proceedings are reported. It is a common file for the 26 Member States of the Schengen area, the aim of which is to pool the alerts of the competent authorities (police forces, border guards) of the various Member States in order to guarantee better cooperation and ensure a high level of security within the territory[293]. It is the most widely used European file in the security context.

This file is composed of two separate systems, a central system and a system at the level of each Member State, called N.SIS, which is linked to the central system. To ensure optimal security of data transfer, an encrypted network allows communication between the central system and the national systems. Each Member State designates an office which has central responsibility for the N.SIS II. Data is collected, updated, deleted and consulted through the N.SIS II systems of each Member State. Each Member State transmits its alerts through its N.SIS II office and the data entered in the SIS is derived from the national police files.

At the European level, the SIS is placed under the aegis of the European Agency for the operational management of large-scale information systems (eu-LISA), which is responsible for the operational management of the central SIS and the monitoring and security of the communication infrastructure, as well as for coordinating relations with the EU countries[294].

As for access to the file, it is very limited. Only legally designated competent national authorities responsible for border controls, police and customs controls, prosecution in criminal proceedings and judicial enquiries, prior to indictment or charge, visas and residence permits are entitled to access it. Europol can search the database but requires the permission of the member country concerned before it can use the data. Eurojust National Members and their assistants also have the right to consult the data. Users can only access the data necessary for the performance of their tasks[295]

A strict framework is established within the SIS to ensure the protection of data subjects. In order to ensure the coordination of the protection of personal data in the framework of the SIS II file, representatives of the national data protection authorities of all Schengen member states and the EDPS meet twice a year in a working group called the Schengen Information System II Supervision Coordination Group ("SIS II SCG")[296]. The information of the data subjects, a central principle of the Law Enforcement Directive, remains, in the framework of this file, at the discretion of each national

---

[293] EUROPEAN PARLIAMENT AND COUNCIL, *Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II),* 20 décembre 2006, *JOUE L 381 of 28 December.2006, p. 4–23,*
[Online] Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006R1987

[294] EU-LISA, "SIS The most widely used IT system for security and border management in Europe" [Online] Available: https://www.eulisa.europa.eu/Publications/Information%20Material/Leaflet%20SIS.pdf

[295] List of competent authorities which are authorised to search directly the data contained in the second generation Schengen Information System pursuant to Article 31(8) of Regulation (EC) No 1987/2006 of the European Parliament and of the Council and Article 46(8) of Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System, 14 July 2017, JOUE C 268/1, 27 July 2016,
[Online] Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017XC0714%2802%29

[296] EDPB, Schengen Information System II Supervision Coordination Group (SIS II SCG), [Online] Available: https://edps.europa.eu/data-protection/european-it-systems/schengen-information-system_fr

authority, each one having the power to decide what information can be revealed or not[297]. The SIS file, which centralises data from several countries, poses the problem of how people can exercise their rights if they do not know which authority to turn to because they do not have sufficient information.

Despite the efforts to protect the individuals, in 2018 the European Parliament adopted three new regulations extending the scope of the SIS II file by including even more sensitive data on individuals. The strengthening of security in the general interest is done at the expense of individuals who see their fundamental rights diminished. Indeed, the regulations adopted on the use of the SIS in the field of police and judicial cooperation in criminal matters[298], in the field of border checks[299] and for the purpose of returning illegally staying third-country nationals[300] introduce, in addition to new categories of alerts, the possibility of using biometric data such as facial images for identification purposes, in particular to ensure the consistency of border control procedures. They also allow the inclusion of DNA profiles to facilitate the identification of missing persons where fingerprints, photographs or facial images are not available or do not allow identification. Access to the data is also more open, allowing Europol to access all categories of data and to exchange additional information with Member States' SIRENE offices. Furthermore, in case of a hit if a person is wanted in connection with a terrorist offence, the competent national authorities are obliged to inform Europol.

5.2.4 The SIRIUS platform

In response to increasing requests for access to electronic evidence by European law enforcement agencies outside their territory, the SIRIUS project was created in late 2017 to address this need[301]. Created by Europol's European Counter-Terrorism Centre and European Cybercrime Centre, in partnership with Eurojust and the European Judicial Network opens up access to pooled resources for European law enforcement and judicial authorities. In the context of our study, we will focus on the provision of access to electronic evidence held by online service providers for law enforcement[302]. This is done on the Europol Expert Group (EPE) platform, which ensures the security of the data hosted on it while allowing access by the various authorised authorities. Indeed, as the platform is supposed to host only non-personal data allowing collaboration and knowledge sharing

---

[297] EUROPEAN PARLIAMENT AND COUNCIL, *Regulation (EC) n°1987/2006, op cit,* Recital 15.

[298] EUROPEAN PARLIAMENT AND COUNCIL, *Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU,* 28 November 2018, PE/36/2018/REV/1, JOUE L 312 of 7 December 2018, p. 56–106, [Online] Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32018R1862

[299] EUROPEAN PARLIAMENT AND COUNCIL, Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006, 28 November 2018, PE/35/2018/REV/1, JOUE L 312 of 7 December 2018, p. 14–55, [Online] Available: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32018R1861

[300] EUROPEAN PARLIAMENT AND COUNCIL, Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals, 28 November 2018, PE/34/2018/REV/1, JOUE L 312 of 7 December 2018, p. 1–13, [Online] Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32018R1860

[301] SIRIUS Project, SIRIUS Cross-Border Access to Electronic Evidence, [Online] Available: https://www.europol.europa.eu/operations-services-and-innovation/sirius-project

[302] EUROPOL, *SIRIUS EU Digital Evidence Situation Report*, 2ndAnnual Report, 2020, [Online] Available: https://www.europol.europa.eu/cms/sites/default/files/documents/sirius_desr_2020.pdf

between Europol Member States[303], the SIRIUS project benefits from a partitioned space maximising data security and whose access is limited to judicial and law enforcement authorities[304].

Beyond the challenges posed by international cooperation in terms of infringing on the fundamental right of individuals to the protection of their personal data, the SIRIUS project has the particularity of integrating, within the framework of the cooperation that it allows, private actors such as online service providers. Since its kick-off meeting, representatives of Internet giants such as Facebook, Google, Microsoft, Twitter and Uber have been involved in the project and were present alongside the governments[305]. The aim is to strengthen judicial cooperation between the United States and the European Union in terms of access to electronic evidence, particularly as these large digital companies are essentially American and the current legal framework is not efficient. The United States, a third country to the European Union, is not subject to the regulation on personal data and no longer benefits from a decision on the adequacy of the regulation in force concerning data[306]. Nevertheless, as the European regulation has an extraterritorial vocation, American companies are subject to it as long as they process data of European citizens or are located on European soil. Consequently, the latter are supposed to ensure effective protection of the personal data they hold. However, the transfer of data by these companies to third parties, outside the framework of the purposes established for their processing, constitutes non-compliance with the GDPR. A conflict then arises between responding to the authorities' request and protecting the data of the persons concerned.

Nevertheless, judicial authorities benefit from the "authorised third party" exception and have the power to require data controllers to disclose personal data. To do so, conditions are well defined. Firstly, the request must be in writing and specify the legislative grounds for it, the request must concern persons who are identified or identifiable by name, and the authorised third party may not have access to an entire file.

Its request must be ad hoc and must specify the categories of data it wishes to access. However, the E-evidence project of 17 April 2018[307], which is supposed to harmonise at European level the fact of allowing, while protecting personal data, the competent authorities to be provided with digital evidence, thanks to data stored in the cloud, has still not been adopted. As criminal proceedings are a matter of national sovereignty, each state has its own legislation on the matter and will therefore have to justify its desire to access data on the basis of its national laws. If the communication of data to a State, an authorised third party, is justified, there is no justification for the processing that will be carried out by sharing this data with the other judicial authorities that are members of the SIRIUS project, the aim of which is to centralise requests to online service providers in order to accelerate proceedings.

[303] Europol platform for experts, [Online] Available: https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-platform-for-experts

[304] SIRIUS, Section « Adhésion et accès » [Online] Available : https://www.eurojust.europa.eu/sirius

[305] EUROPOL, « Europol launches the SIRIUS platform to facilitate online investigations », 31 October 2017, [Online] Available : https://www.europol.europa.eu/media-press/newsroom/news/europol-launches-sirius-platform-to-facilitate-online-investigations

[306] CJEU, 16 July 2020, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems ("Schrems II"), Case C-311/18 [Online] Available: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.html

[307] EUROPEAN PARLIAMENT AND COUNCIL, Proposal for a Regulation of The European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, 17 April 2018, COM/2018/225 final - 2018/0108 (COD), [Online] Available : https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2018%3A225%3AFIN

5.3 Type of data collected

The various categories of data may imply different treatment by existing rules and different procedures for accessing them. Each of the above categories may contain personal data and are therefore covered primarily by the provisions of the Law Enforcement Directive. However, the intensity of the impact on fundamental rights varies between them, in particular between metadata on the one hand and data content on the other. Appropriate safeguards must be provided depending on the level of sensitivity. The sensitivity of the data may also depend on the volume requested; large volumes of specific types of metadata may allow for the profiling of individuals, in particular with regard to location, and therefore require more safeguards than smaller amounts or different types of metadata.

There are two main categories of data that will be of interest to investigators in their work: non-content data and content data.

5.3.1 Non-content data

Online activities and communications generate data, which is not limited to the content (i.e., text, picture, audio, video, etc.), but also generate non-content data as traffic data about the communication itself and the device, known as metadata; its location, and information for user identification. Some of the non-content data is personal data, but even non-personal non-content data can be identifying if combined, and thus have an impact on privacy.

Connection data is subject to a retention obligation by European telecommunication operators for reasons of crime-fighting and national protection. This connection data is thus included in non-content data. This data, as explained above, provides information on certain aspects of other data (e.g. date and time of creation, source of the data, file size, etc.). This is information data about the context of communications between individuals, but not the communications themselves, will not bring a question of infringement of the confidentiality of correspondence itself, even if it can be an issue for privacy.

The CJEU listed the different connection data in its judgment of 6 October 2020 at paragraph 82: "the data which those regulations require providers of electronic communications services to retain are, in particular, those necessary to trace the source of a communication and its destination, to determine the date, time, duration and type of the communication, to identify the communications equipment used and to locate terminal equipment and communications, data which include, in particular, the name and address of the user, the telephone numbers of the caller and the called party and the IP address for Internet services. However, this data does not cover the content of the communications concerned"[308].

[308] CJEU, 6 October 2020, aff. Jointes C-511/18, C-512/18 et C-520/18, point 82, [Online] Available : https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=13137602

Subscriber data	Name Address Telephone number Username	E-mail address Payment information ID number Date of birth
Identification data	IP address Port number for dynamic IP address SIM number Device identification numbers such as IMEI	
Geolocation data	Location of the equipment or line at the start of the communication Location of the equipment or line at the end of the communication	
Traffic data	Date and time of communication Duration of communication Start of communication End of communication Data volume of communication	Type of network technology Type of communication Missed calls Connection to the service Disconnection from the service
	Identifiers of the account/device to which the communication was forwarded or transferred Identifiers of the account/device to which the communication was attempted to be forwarded or transferred Identifiers of the account/device to which the communication was sent	

5.3.1.1 Connection and traffic data

This is the non-content data which includes data about the connection, traffic or location of the communication (e.g. IP or MAC addresses). Access logs, which record the time and date a person accessed a service, as well as the IP address from which the service was accessed.

It is important to note that for the CJEU these data are just as sensitive as the content of private correspondence itself. It notes that metadata provide "the means of establishing (...) the profile of the persons concerned, information which is just as sensitive, with regard to the right to respect for private life, as the actual content of communications"[309].

In France, from an administrative point of view, the 2015[310] *Loi sur le Renseignement* (Intelligence Act) and its application decree[311] provide a framework for the conditions under which French intelligence services are authorised to access traffic data, a framework provided for in the Internal Security Code[312].

In France, access to such data can only be granted in a regulated manner through the use of a requisition. The Code of Criminal Procedure provides a framework for requisitions for stored data via Articles 60-1, 77-1-1 and 99-3 of the Code of Criminal Procedure. The requisition is thus well defined by Article 77-1-1 of the Code of Criminal Procedure (preliminary investigation):

> *The public prosecutor or, with the latter's authorisation, the judicial police officer or agent may, by any means, request any person, private or public establishment or body or public administration likely to hold information relevant to the investigation, including information from a computer system or nominative data processing, to hand over such information to him or her, in particular in digital form, where applicable in accordance with the standards laid down by regulation, without being able to invoke the obligation of professional secrecy without legitimate reason.*

These articles allow public authorities to request, under certain conditions and in the context of their missions, stored data from any person, private or public institution or body, or public administration, without informing the data holder(s) in advance. This requisition may only be made on the basis of a specific, written and reasoned request, targeting named persons, identified directly or indirectly, or other digital resources.

For Germany, traffic data, such as connection numbers or identifiers, location data of a phone, can be obtained under Section 100g of the German Code of Criminal Procedure, which regulates the collection of traffic data. However, such collection is only possible when a significant criminal offence is committed. A court order is also required to carry out this type of collection[313].

---

[309] CJEU, 6 October 2020, joined Cases C-511/18, *La Quadrature du Net and Others*, *op. cit.*

[310] French Code of intelligence, no. 2015-912 of 24 July 2015 [Online] Available : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030931899/

[311] Decree no. 2016-67 of 29 January 2016 on intelligence gathering techniques, [Online] Available : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000031940885/.

[312] Article L. 851-1 and subsequent articles of Internal Security Code, [Online] Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030935595.

[313] Article 100g of the German Code of criminal procedure « Strafprozeßordnung », [Online] Available : https://dejure.org/gesetze/StPO/100g.html.

The main tool for cross-border exchange of information is **the** European Investigation Order ("**EIO")**, based on Directive 2014/41/EU[314] and used by all Member States of the EU, except for Ireland. Recital 30 of the Directive states that "*possibilities to cooperate under this Directive on the interception of telecommunications should not be limited to the content of the telecommunications, but could also cover collection of traffic and location data associated with such telecommunications, allowing competent authorities to issue an EIO for the purpose of obtaining less intrusive data on telecommunications*." Requests for accessing non-content data in another Member State follow the same legal procedure as those at national level, except through an EIO.

Another strong instrument is EU's **Convention of 29 May 2000 on Mutual Assistance in Criminal Matters** ("2000 Convention"). It's the main legal tool for judicial requests to other Members of the Council of Europe[315]. It should be noted that the EIO and the 2000 Convention are the strongest channels for the exchange of non-content data for most of the LEA, as per the *Study on the retention of electronic communications non-content data for law enforcement purposes*[316].

Another way to obtain cross-border data is the **Council of Europe's Cybercrime contact point**, established by Article 35 of the Budapest Convention on Cybercrime. This point of contact is used by LEA respondents that deal principally with cybercrime issues. This instrument is used in the fields of confidentiality, integrity and availability of computer data and systems, computer-related forgery and fraud, but also for the investigation and prosecution of child sexual exploitation and child pornography, and copyright infringement.

Finally, other **specialised frameworks** for the exchange of information are the Naples II Convention in the field of cooperation between EU customs administrations, and Memoranda of Understanding of the European Securities and Markets Authorities (ESMA) and of the International Organization of Securities Commissions (IOSCO). These international cooperation tools are used by specialised national authorities, which are granted access to non-content data in the national legislative framework of data conservation, which is the Authority for Financial Markets (*Autorité des Marchés Financiers*) in France.

The aforementioned study has reported that the excessive length to obtain the non-content data, as well as the lack of harmonised rules and the lack of knowledge of other states' data access practices, threatens and makes it difficult for LEAs to obtain these data from other states[317].

5.3.1.2 Subscriber data

This type of data is defined by Article 18 of the Convention on Cybercrime, and 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"*
According to this same article, that kind of data allows to establish:

314 EUROPEAN PARLIAMENT AND COUNCIL, Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, 3 April 2014, *op. cit.*

315 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, Official Journal C 197, 12.7.2000, pp. 1-2, [Online] Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000F0712%2802%29.

316 European Commission, Directorate-General for Migration and Home Affairs, Dupont, C., Cilli, V., Omersa, E., et al., *Study on the retention of electronic communications non-content data for law enforcement purposes: final report*, Publications Office, 2020, [Online] Available： https://data.europa.eu/doi/10.2837/384802

317 *Ibid.* p. 92-93.

(a) the type of communication service used, the technical provisions taken thereto and the period of service;
(b) 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;
(c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.[318]

In other words, this is data that allows the identification of the subscriber to a communication (e.g. name, address, user name, telephone number). It should be noted that in Spain, unlike other partner countries, this also includes information such as identification number, nationality and date of birth[319].

5.3.1.3 Geolocation data

According to EU legislation, mobile location data may, in principle, only be processed if it is anonymised or processed with the consent of the data subject[320]. Nevertheless, the ePrivacy Directive provides by way of exception that Member States may take specific legislative measures to derogate from the former rule for the purpose of safeguarding public security[321].

However, the legislative measures in question, which would allow the use of non-anonymised location data without the consent of individuals, must be necessary, appropriate and proportionate to the public security risk involved. Thus, such measures cannot be implemented without appropriate safeguards.

Thus, in the context of a French judicial police investigation, it is possible, in accordance with Articles 230-32 to 230-44 of the Code of Criminal Procedure, to locate in real time any vehicle or object of a person suspected of having committed a crime or an offence punishable by more than three years imprisonment.

However, metadata is considered to be a 'silent trace' that can provide additional or even decisive information in the context of a judicial investigation. In France, an expert from the Ministry of the Interior's IT-electronic department has therefore developed an application that allows any investigator to quickly exploit such data, especially geolocation data, GENDEXIF[322].

5.3.2 Content data

The Budapest Convention does not define this type of data; however, it provides a high level of privacy protection for the interception of content data. Accordingly, the power to intercept content data must be applied to "a range of serious offences to be determined by national law"[323]. The interception of content data is therefore governed by the applicable national laws.

---

[318] Article 18 of the Budapest Convention on Cybercrime.

[319] European Commission, Directorate-General for Migration and Home Affairs, Dupont, C., Cilli, V., Omersa, E., et al., *Study on the retention of electronic communications non-content data for law enforcement purposes: final report*, Publications Office, 2020, *op. cit.*, p. 48.

[320] Article 9 of the 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 ("ePrivacy Directive"), 12 July 2002, [Online] Available : https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

[321] *Ibid.,* article 15.

[322] Pôle judiciaire de la gendarmerie nationale IRCGN - SCRCGN, « Geolocation data analysis with GendExif », [Online] Available : https://www.gendarmerie.interieur.gouv.fr/pjgn/innovation/les-brevets-et-innovations/l-analyse-de-donnees-de-geolocalisation-avec-gendexif

[323] Article 21 of the Budapest Convention on Cybercrime.

This may include the text of an email, a message, a blog or an article, videos, images, sounds stored in a digital format. Content data is defined by reference to the principle of confidentiality of correspondence which applies to electronic mail. Under Article L. 32-3 of the French Post and Electronic Communications Code, confidentiality covers the content of the communication, the identity of the correspondents, the title of the message and the documents attached to the communication.

Third Parties Personal data:

As the large volumes of data extracted from smartphones are likely to contain information on the private lives of the owner of the device, it is also very likely that they contain personal information about third parties, such as the owner's family and friends, and contacts in general.

In other words, it is not only the data of the device owner that is processed by LEAs, but also the data of third parties who have a relationship with the device owner or simply whose contact details or other information the device owner has added to his or her smartphone. Although this presents a very significant risk of over-processing, **no specific rules on this issue were found in this study**. As long as such processing is not regulated and no clear limits are set, there is a high risk of disproportionate intrusion into the privacy of third parties. This could even affect the willingness of victims and witnesses to come forward and report serious crimes.

However, Article 6 of the Law Enforcement Directive requires LEAs to make, where appropriate and to the extent possible, a clear distinction of the data of third parties who have been mentioned in the Directive as "persons who may be called as witnesses in investigations relating to criminal offences or subsequent criminal proceedings, persons who may provide information on criminal offences, or contacts or associates of any of the persons referred to in (a) and (b)". However, according to the Directive, this distinction will be respected "as far as possible" without specific safeguards that make it difficult to comply with this provision in a practical and uniform manner.

Despite the absence of a specific provision, it is still possible to apply the data processing principles to third party data. According to the principle of proportionality and relevance, the data processed must be strictly necessary for the purpose of the file. In other words, the personal data collected must not be excessive in relation to its purpose.

From the perspective of this principle, third party data that is not relevant for an investigation must be considered as 'excessive' data and should therefore not be collected in the first place. However, in practice this is not so simple, for example in the case of the extraction of an SMS between the owner of the device and another person. An important question in this respect is whether or not it is possible to extract only specific data from an SMS message. In general, the technology used by LEAs does not allow selecting a specific piece of data to be extracted today. As stated in the ICO[324] study, the specific technologies for extracting data from mobile phones are also another determining factor for lawful data processing during investigations. processing of data during investigations.

Therefore, the absence of specific and harmonised rules in this area may lead to inconsistencies in the practices of retention, disclosure and security of extracted data. Thus, a specific legislative framework for the extraction and processing of third party data should ensure clear and predictable measures in this respect.

In this regard, an important decision was recently issued by the EDPS[325], which shows the willingness of the European institutions to regulate the processing of data of third parties who are not involved in and linked to a crime.

[324] ICO, "Mobile phone data extraction by police forces in England and Wales", June 2020, p. 45, [Online] Available : https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/

[325] EDPS Decision on the retention by Europol of datasets lacking Data Subject Categorisation, 3 January 2022 (Cases 2019-0370 & 2021-0699)

In his recent decision, the EDPS set a specific retention period for Europol, concerning the deletion of data belonging to third parties that are not linked to any criminal activity. Thus, Europol is not allowed to keep the personal data of such persons for more than 6 months.

The EDPS calls the issue of excessive data collection "Europol's Big Data challenge" and underlines that "the storage of large volumes of data without categorisation of the data subjects" endangers the fundamental rights of individuals. The importance of this issue had been reminded to Europol in September 2020 by the EDPS, who even asked Europol to define a proportionate data retention period for filtering and retrieving collected personal data according to Regulation (EU) 2016/794 ("Europol Regulation").

However, Europol did not comply with the EDPS' requests and the EDPS therefore concluded that Europol's data processing practices violate the principles of data minimisation and purpose limitation, which are laid down in the Regulation.

5.3.3 Cross-referencing of personal data

Although metadata, apart from subscriber data, does not generally appear to contain personal data, it can very easily become personal data due to data combining techniques. These techniques are based on cross-referencing and linking different data of a data subject and require special attention from LEAs regarding the use of the data.

This data, taken together, may provide information about the private lives of the individuals whose data has been retained, which may not be relevant to the investigation. Examples may vary depending on the evidence sought, but by way of example, this could be the case with daily life habits, activities carried out, social relationships of these individuals, the social environments they frequent and data from third parties that have no connection with the investigation being conducted.

On this issue, the Information Commissioner's Office (ICO) in the United Kingdom has taken a stricter approach in its report entitled "Mobile phone data extraction by police forces". In this report, it was stated that personal data accessible through a smartphone is diverse in nature and generally includes intimate and private communications between individuals and is clearly likely to meet one or more criteria of sensitive data. Therefore, according to the ICO, as LEAs cannot be certain of the nature of the data before accessing it, they should assume that it is sensitive and ensure that they comply with the specific requirements of sensitive data[326].

The ICO approach could be questionable as restrictive from the perspective of the law enforcement agencies. However, it should be noted that, in order to avoid excessive data processing, especially the principle of purpose as well as proportionality must always be taken into account. The approach of 'extracting as much data as possible' should be avoided in all circumstances in line with the basic principles of the RGPD and the Law Enforcement Directive.

5.4 Data retention

5.4.1 Retention of data by telecommunication operators

5.4.1.1 General provisions

In the Netherlands, the data collected fall within the exception of police missions and are subject to the Police Data Act: the Wet Politiegegevens (WPG)[327], which concerns processing in the context of investigations for the maintenance of public order, and for the prevention of dangers and serious violations of public order. No distinction is made between sensitive and non-sensitive data.

[326] *Ibid.,* p. 33-34.

[327] See: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/politie-justitie/politie

Data are kept in principle for 5 years and then deleted[328]. Data may not be deleted insofar as the authorities need them for the performance of their tasks.

In Germany, stored data can be secured and preserved in order to maintain the evidence chain and to exclude manipulation in accordance with Sections 94 and 98 of the Code of Criminal Procedure[329], provided that a criminal offence is suspected and, as a rule, a court order has been issued. However, a judicial backup of the stored electronic evidence must be made. For this purpose, a 1:1 bit-by-bit copy of the data, including the forensic checksum, is produced in a standardised format, so that a write protection module specifically used for this process ensures that access to the source data is always read-only. After this duplication ("imaging") process, a new verification takes place using the stored checksums. The integrity of the secured data is thus ensured by the calculation of a cryptographic checksum. This produces a backup copy that can be used in court and is the basis for all subsequent investigations.

These investigations are carried out exclusively on the forensic copies and never on the original data.

In order to be retained, the data must also be cloned in Spain. Article 7 of the Spanish law on data protection, which deals with data that are subject to 'special protection', i.e. sensitive data, states that 'personal data relating to the commission of criminal or administrative offences may form part of the automated files of the competent public administrations, in the cases provided for in the regulations governing such files'[330].

In a practical guide on the use of personal data in the police sector drafted by an advisory committee of the Council of Europe published in 2018, recommendations were made regarding the retention of personal data. In this respect, it is mentioned that retained data should be correct, up-to-date, necessary, relevant and not excessive in relation to the purposes for which they were collected. Therefore, clear rules must be put in place regarding the processing of the different databases. Furthermore, the necessity principle must be applied throughout the life cycle of the processing. Storage may be allowed if the analysis shows that the personal data are necessary for police purposes, however, the grounds for storing and processing the data should be reviewed periodically.

On the periods of data retention, they should be regulated in national or international law. The Committee gives an example that if the law relating to a specific crime provides for a 4-year data retention period, and if personal data are processed by the police only in relation to that crime beyond 4 years after collection, and there is no reason for this, then the retention of the data in question would be considered illegal.

However, in order to comply with the legislation and at the same time ensure the efficiency and success of an investigation, it is strongly recommended that police forces develop internal procedures and/or guidelines that set out the length of time personal data should be retained or the need for retention reviewed on a regular basis.

To illustrate his point, it adds that if the law prescribes a data retention period of 4 years, but the person under investigation is acquitted of all charges after 2 years, his data should be deleted from the database (if he is not a repeat offender or if there is no other information to indicate that he has committed a crime of the same category again and if all appeal periods have expired), provided that all review periods for the case have also expired. Similarly, if the investigation is still ongoing after 4 years and the data on that person is still relevant, the police should be able to retain it.

[328] Article 14 of the Dutch Police Data Act (« WPG »).

[329] German Code of criminal procedure, [Online] Available : https://www-gesetze--im--internet-de.translate.goog/stpo/?_x_tr_sl=de&_x_tr_tl=fr&_x_tr_hl=fr&_x_tr_pto=sc

[330] Article 7 of the Spanish Law on data protection, [Online] Available : https://bittemple.es/legislacion/lopd-151999/titulo-ii-principios-proteccion-datos/lopd-articulo-7-datos-especialmente-protegidos/

In the latter case, it is important to design the retention strategy in such a way that the data used in the criminal proceedings remain available to the controller until the end of the legal proceedings (i.e. all avenues of appeal have been exhausted or all time limits for appeal have expired).

The police should have systems and mechanisms in place to ensure that the data recorded are accurate and that their integrity is maintained.

Personal data collected by the police for administrative purposes should be kept separate (as far as possible logically and physically) from data collected for police purposes. The police may access it where necessary and permitted by law.

In November 2020, the Council of the European Union adopted a draft resolution that seeks to oblige operators of secure messaging systems such as WhatsApp or Signal to allow intelligence services to access content exchanged via privileged access. This draft has not yet been adopted.

Articles 56 and 57 of the French Code of Criminal Procedure about seizure of documents **do not apply when the medium analysed belongs to a victim or witness or does not have an identified owner**, as the technical findings or examinations will always guarantee the authenticity of the medium and the integrity of the original data.

On the other hand, Article 56 of the Code of Criminal Procedure allows for the exploitation of the computer object on the spot during the search in order to verify that it does indeed belong to the person being searched so that objects belonging to third parties are not exploited and their personal data not extracted.

5.4.1.2 Traffic and connection data

As regards the retention of geolocation data by telephone operators, in France Article L34-1 of the French Post and Electronic Communications Code states that operators must retain their users' connection data for one year in order to make them available to the judicial or police authorities for the purposes of investigating, establishing and prosecuting criminal offences.

However, the article specifies that the data kept and processed relate exclusively to the identification of persons using the services provided by the operators, to the technical characteristics of the communications provided by the latter and to the location of the terminal equipment and may in no case relate to the content of the correspondence exchanged or the information consulted, in any form whatsoever, in the context of these communications.

According to the European Commission's report[331], national laws in EU Member States provide for different retention periods for metadata retained by electronic communications service providers, which also vary depending on the purpose of their retention. In practice, it has been found that LEAs find it difficult to know which metadata will be available for consultation.

Member States often provide for a longer retention period for subscriber data than for traffic, identification and location data. As subscriber data are necessary for the service contract between customers and electronic service providers, these types of data are kept for the duration of the contract[332].

In France and Spain, where there is a legal obligation to retain metadata for law enforcement purposes, the metadata retention period for traffic, identification and location data is 12 months.

[331] European Commission, Directorate-General for Migration and Home Affairs, Dupont, C., Cilli, V., Omersa, E., et al., *Study on the retention of electronic communications non-content data for law enforcement purposes: final report*, Publications Office, 2020, *op. cit.*

[332] *Ibid,* p. 52.

However, on 6 October 2020, the CJEU issued two very important decisions on data retention[333]. The objective of the Court was to examine the conformity with EU law of certain regulations adopted by Member States (notably France, Belgium and the UK) providing for the obligation for electronic communications service providers to retain user data and transmit them to certain public authorities for the purpose of fighting crime or safeguarding national security. In order to protect fundamental rights and freedoms, the CJEU in these two decisions opposed the mass collection of internet and telephone connection data by States.

Before explaining the substance of the judgment, it is worth remembering that in 2016 the CJEU ruled that Member States could not impose a "general and indiscriminate obligation" on electronic communications service providers to collect and retain traffic and geolocation data[334].

Indeed, according to this European case law, data on Internet connections and telephone conversations could therefore theoretically no longer be retained by electronic communications service providers. However, several EU states continued to require such collection in order for LEAs to access them. This was the case in France, where electronic communications service providers were obliged to retain all user metadata for one year, in accordance with Decree No. 2011-219 of 25 February 2011[335]. The data retained in France is all metadata except the content of the message itself, which would require interception.

The CJEU ruled on the unlawfulness of "generalised and undifferentiated" metadata retention practices and thus confirmed its 2016 decision, mentioned above. In its 2020 decision, the Court ruled that legislative measures imposing on electronic communications service providers, as a preventive measure, a generalised and undifferentiated retention of traffic and location data is contrary to Union law as it entails a particularly serious infringement of the fundamental rights guaranteed by the Union Charter. However, the Court accepted the case of a "serious threat to national security which is actual or foreseeable" with data retention "limited in time to what is strictly necessary" as an exception. In its second judgment, (C-623/17), which concerned the UK in particular, the CJEU confirmed that national regulations cannot require providers of electronic communications services to "transmit or retain customer connection data in a general and indiscriminate manner"[336].

Following these CJEU rulings, three new decrees were published on 20 October 2021 in France, which specify the framework applicable to the retention of connection data by electronic communications operators.

[333] CJEU, 6 October 2020, Case C-623/17, *Privacy International*, and in Joined Cases C-511/18, *La Quadrature du Net and Others*, C-512/18, *French Data Network and Others*, and C-520/18, *Ordre des barreaux francophones et germanophone and Others*, *op. cit.*

[334] CJEU, 21 December 2016, joined cases C203/15 and C698/15, §76 et seq., [Online] Available : https://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=EN

[335] De Gaulle Fleurance and Associates, « The Court of Justice of the European Union sets limits to mass surveillance », 27 October 2020, [Online] Available : https://www.degaullefleurance.com/en/the-court-of-justice-of-the-european-union-sets-limits-to-mass-surveillance/#_ftn1 [Accessed 5 January 2022].

[336] CJEU, Decision Privacy International C-623/17 of the Court of Justice of the European Union, *op. cit.*

Article 17 of Law 2021-998 of 30 July 2021 on the prevention of terrorist acts and intelligence modified the framework for the retention of connection data by electronic communications operators. This provision specifies the list of data that must be retained and refers to the adoption of several decrees:

- the first (No. 2021-1361, 20 Oct. 2021) relates to the categories of data kept by electronic communications operators, pursuant to Article L. 34-1 of the French Post and Electronic Communications Code;

- the second (No. 2021-1363, 20 Oct. 2021) provides for the possibility of ordering electronic communications operators to retain traffic and location data for a period of one year in order to safeguard national security.

According to Article L. 34-1 of the French Post and Electronic Communications Code:

> Electronic communications operators, and in particular persons whose activity is to offer access to online public communication services, shall delete or render anonymous data relating to electronic communications.

As for the data that may be retained, according to the said article, they are classified into six categories.

The first category relates to information on civil identity. This must be kept "for the purposes of criminal proceedings, the prevention of threats to public security and the safeguarding of national security" by electronic communications operators for a period of five years from the end of the validity of the contract.

Similarly, for the same purposes mentioned above, the categories including information collected at the time of the subscription of a contract or the creation of an account and information relating to payment are kept for a period of one year from the end of the validity of the contract or the closure of the account.

"For the purposes of combating crime and serious delinquency, preventing serious threats to public security and safeguarding national security", technical data enabling the source of a connection to be identified or data relating to the terminal equipment used must be kept for one year from the time of connection or use of the terminal equipment.

Other traffic and location data may also be retained for one year if several conditions are met. This operation requires an injunction from the Prime Minister, who takes such a measure for reasons relating to the safeguarding of national security, when a serious, current or foreseeable threat to national security has been established. The same data may be the subject of a rapid preservation order by authorities with access to electronic communications data for the purposes of preventing and punishing crime, serious delinquency and other serious breaches of the rules they are responsible for ensuring compliance with, in order to access such data.

Lastly, the decrees require electronic communications operators to keep information enabling them to locate communications made via mobile telephones and require hosts to keep information on the content created[337].

[337] Decrees numbered 2021-1361 and 2021-1363 of 20 October 2021 ; Editions Législatives, « Du nouveau sur la conservation des données de connexion », 5 November 2021, [Online] Available : https://www-editions-legislatives-fr.ressources-electroniques.univ-lille.fr/actualite/du-nouveau-sur-la-conservation-des-donnees-de-connexion

5.4.2 Duty of cooperation of telecommunication operators

Cooperation obligations have been set up by the different national law of Exfiles partner countries; the table below summarizes them.

Table 5: Obligation of telecommunications service providers to assist the authorities

Obligation of telecommunications service providers to assist the authorities	
France	Article D98 of the Code des postes et des communications électroniques (CPCE)[338]: "III. - The operator shall put in place and ensure the implementation of the means necessary to respond to requests made in the context of: - judicial digital investigations formulated pursuant to articles 60-1, 74-1, 7-1-1, 99-3, 100 to 100-8, 230-32 to 230-34, 706-95, and 709-13 of the code of criminal procedure; - information provided pursuant to Book VIII of the Code de la sécurité intérieure. *Article 57-1 of the Code Pénal*: Judicial police officers may, by any means, request any person likely: 1° To have knowledge of the measures applied to protect the data to which access is permitted in the context of the search; 2° To provide them with information allowing access to the data mentioned in 1°.[339] Encryption keys may be required if the content is not plaintext. Article 230-1 of the Code de procédure pénale: Without prejudice to the provisions of Articles 60, 77-1 and 156, where it appears that data seized or obtained in the course of the investigation or enquiry have been subject to transformation operations that prevent access to or understanding of the unencrypted information they contain, the public prosecutor, the investigating court or the court of first instance hearing the case may designate any qualified natural or legal person to carry out the technical operations required to obtain the plaintext version of the information and, where encryption has been used, the secret decryption convention, if this appears necessary. The same article also provides that "If the penalty incurred is equal to or greater than two years' imprisonment and the needs of the investigation or trial so require, the public prosecutor, the investigating court or the trial court hearing the case may prescribe the use of State resources subject to national defence secrecy in the manner provided for in this chapter". Internet operators (in particular access and hosting providers) have obligations

[338] French Postal and Electronic Communications Code, [Online] Available : https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070987/LEGISCTA000006181878/

[339] French Code of Criminal Procedure, *op. cit.*

Obligation of telecommunications service providers to assist the authorities	
	to cooperate regarding identification: they must, on the one hand, inform users (Article 6-I.7 LCEN), and on the other hand, hold and keep "data likely to allow the identification of anyone who has contributed to the creation of the content or of one of the contents of the services of which it is a provider" (Article 6-II LCEN)[340]
Netherlands	Under the Telecommunications Act "*Telecommunicatiewet*" [341], telecommunications service providers are obliged to cooperate in the event of an order under the Code of Criminal Procedure [342], or the *Intelligence and Security Services Act* [343]2017 to intercept or record telecommunications.
Germany	An ordinance on the implementation of telecommunications monitoring measures makes it possible to oblige telecommunications service providers to be able to monitor telecommunications. If the provider uses communication protection measures, or cooperates in the production or exchange of keys, it must be able to decrypt the telecommunications[344]. This does not make it possible to oblige providers to decrypt the encryption measures used by the users themselves.
Spain	Code of Criminal Procedure (LECRIM) updated by Law 13/2015 of 5 October 2015[345]: Article 588 ter a. Pre-requisite: Authorisation for the interception of telephone and telematic communications may only be granted when the subject of the investigation is one of the offences referred to in Article 579.1 of this law or offences committed by means of computer instruments or any other information or communication technology. Article 588b e. Duty to cooperate:

[340] Law no. 2004-575 For Confidence in the Digital Economy (in French « LCEN ») of 21 June 2004, [Online] Available : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164/

341 Article 13.2 of the Telecommunicatiewet, 19 October 1998, [Online] Available : https://wetten.overheid.nl/BWBR0009950/2020-12-21#Hoofdstuk13

342 Article 126m. of the Dutch Code of Criminal Procedure, [Online] Available : https://wetten.overheid.nl/jci1.3:c:BWBR0001903&boek=Eerste&titeldeel=IVA&afdeling=Zevende&artikel=126m&z=2021-05-07&g=2021-05-07

343 Art. 51 ff. of the Intelligence and Security Services Act "*Wet op de inlichtingen- en veiligheidsdiensten 2017",* [Online] Available : https://wetten.overheid.nl/jci1.3:c:BWBR0039896&hoofdstuk=3&paragraaf=3.2&sub-paragraaf=3.2.5&sub-paragraaf=3.2.5.6&sub-paragraaf=3.2.5.6.4&z=2020-01-01&g=2020-01-01

344 Art. 8 (3) of the Ordinance on the Technical and Organisational Implementation of Telecommunications Surveillance Measures "Telekommunikations-Überwachungsverordnung - TKÜV", 3 November 2015, [Online] Available : http://www.gesetze-im-internet.de/tk_v_2005/BJNR313600005.html

[345] Organic Law 13/2015 amending the Criminal Procedure Law for the strengthening of procedural guarantees and the regulation of technological investigation measures, 5 October 2015, [Online] Available : https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10725

Obligation of telecommunications service providers to assist the authorities	
	1. All providers of telecommunications services, access to a telecommunications network or information society services, as well as any person who in any way contributes to facilitating communications by telephone or any other telematic, logical or virtual means or system of communication, shall be obliged to provide the judge, the Public Prosecutor's Office and the judicial police officers designated for the exercise of the measure with the assistance and collaboration necessary to facilitate the execution of intervention orders in telecommunications matters. 2. Subjects required to provide collaboration will be obliged to maintain secrecy about the activities required by the authorities. 3. Obliged subjects who do not comply with the above duties may incur the crime of disobedience. Article 588b i. Access of parties to recordings: 1. Once the secrecy has been removed and the intervention measure has expired, a copy of the recordings and transcripts made shall be given to the parties. If the recording contains data referring to aspects of the intimate life of the persons, only the recording and the transcript of the parts that do not refer to them shall be delivered. The non-inclusion of the entire recording in the transcript issued will be expressly noted. 2. Once the recordings have been examined and within the time limit set by the judge, taking into account the volume of information contained in the media, each of the parties may request the inclusion in the copies of the communications which they consider relevant and which have been excluded. The investigating judge, after hearing or examining these communications himself, shall decide whether to exclude them or to incorporate them into the file. 3. The investigating judge will notify the persons involved in the intercepted communications of the fact of the interference and they will be informed of the specific communications in which they participated that are affected, unless this is impossible, requires a disproportionate effort or may prejudice future investigations. If the notified person so requests, a copy of the recording or transcript of those communications shall be provided to him or her, insofar as this does not affect the right to privacy of others or is contrary to the objectives of the process in which the measure was adopted. The LED is transposed into Spanish law by Organic Law 7/2021, of 26 May 2021, on the protection of personal data processed for the prevention, detection, investigation and prosecution of criminal offences and the execution

Obligation of telecommunications service providers to assist the authorities	
	of criminal penalties[346]: public administrations, as well as any natural or legal person, have a duty to collaborate: they will provide the judicial authorities, the public prosecutor's office or the judicial police with the data, reports, records and supporting documents they request and which are necessary for the investigation and prosecution of criminal offences or for the enforcement of sentences. The request of the Judicial Police must be adapted exclusively to the exercise of the functions entrusted to it by article 549.1 of Organic Law 6/1985, of 1 July, and must always be made in a reasoned, concrete and specific manner, reporting in all cases to the judicial and fiscal authority.
United Kingdom	The Secretary of State may issue a technical capability notice to a telecommunications service provider. This notice may impose obligations, subject to 3 conditions being met: - The Secretary of State must consider that the notice is necessary to ensure that the provider has the capacity to provide the assistance it can provide in relation to interception, obtaining communications data or equipment interference authorised by law - The Secretary of State must consider that the technical advice is proportionate to the purpose of the measure The decision to provide the notice must be approved by a judicial commissioner (a specially appointed judge, who examines the necessity and proportionality of the measure) [347]. The UK Government has put provisions in place to ensure that it receives information in a decrypted format when a warrant has been issued under the IPA and has set forth the removal of encryption from communications via Technical Capability Notice ("TCN"). The Investigatory Powers Act 2016 imposes obligations on telecommunications operators or postal operators through a TCN, to be able to provide assistance in order to remove encryption of the communication or data. Regulation concerning TCN are set forth in the Equipment Interference Code of Practice[348] ; as per its article 8.1., telecommunications operators may be required "to have the capability to provide assistance in giving effect to interception, equipment interference and bulk acquisition warrants and notices or authorisations for the acquisition of communications data. The purpose of maintaining a technical capability is to ensure that, when a warrant, authorisation or notice is served, companies can give effect to it securely and quickly."

[346] Organic Law 7/2021, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and the execution of criminal sanctions, 26 May 2021, [Online] Available : https://www.boe.es/buscar/act.php?id=BOE-A-2021-8806

[347] Investigatory Powers Act 2016, *op. cit.,* section 253.

[348] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf

Obligation of telecommunications service providers to assist the authorities	
	However, TCN does not itself require the "operator to remove encryption per se. Rather, it requires that operator to maintain the capability to remove encryption when subsequently served with a warrant or given a notice or authorisation"[349]. The objective of these dispositions is to ensure that the telecommunication operators has the technical means to remove the encryption in order to give effect a warrant issued under the IPA.
Norway	The Intelligence Services Act 2020 includes a section, not yet in force and still under discussion, which would impose a duty of facilitation on telecommunications service providers, but also on providers of publicly available internet messaging. This duty is characterised by making communication flows available[350], while facilitating search, selection, filtering, testing or storage. In particular, it is expected that the providers of these services will guarantee impeded access by encryption on its part (which does not include encryption services of other parties).

5.4.2.1 Retention of connection data and interference with the privacy of individuals

The collection of this metadata can reveal very sensitive information about individuals, even if the content of the communications is not involved. French MP Isabelle Attard wanted to testify to the sensitivity of this data during parliamentary debates:

> *"For example, you logged on to a swinger or fetish dating site twice a day for a month, but - we are told - we have no idea what you wrote or read... Another example: you called Sida Info Service for twelve minutes, then a medical analysis laboratory for two minutes. A week later, the laboratory called you back. We don't know what you said to each other, but they called you back, and then you called your doctor for fifteen minutes, but again, we don't really know what you talked about."* [351]

The CJEU is aware of the profound interference with privacy that this obligation to retain connection data entails, as underlined in the *Digital Rights Ireland* case of 8 April 2014 in its point 117: "*Taken as a whole, such data may make it possible to draw very precise conclusions concerning the private lives of the persons whose data have been retained, such as the habits of daily life, the places where they are permanently or temporarily staying, their daily or other movements, the activities they engage in, the social relations of those persons and the social circles they frequent. In particular, these data provide the means to establish the profile of the persons concerned, information which is just as sensitive, with regard to the right to privacy, as the content of the communications themselves*.

[349] Article 8.2. of the Investigatory Powers Act 2016.

[350] Intelligence Services Act "*etterretningstjenesteloven*", 19 June 2020, art. 7.2. Online] Available : https://lovdata.no/lov/2020-06-19-77/§7-2 ; ECHR, 25 May 2021, Case of Big Brother Watch and Others v. the United Kingdom, [Online] Available : https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210077%22]}

[351] ATTARD Isabelle, National Assembly, Discussion of the Intelligence Bill, 14 April 2015, [Online] Available : https://www.assemblee-nationale.fr/14/cri/2014-2015/20150215.asp

Attempts have been made to introduce specific regimes for the retention of such data by telecommunications operators and Internet service providers. However, some provisions have been challenged by the case law in the name of fundamental rights and respect for data protection, leading to some conflicts of interpretation between Member States. Therefore, some harmonisation solutions could be envisaged in this respect.

Firstly, a Directive of 15 March 2006 on the length of retention[352] provides for a **minimum period of retention of 6 months** and a **maximum period of 2 years from the** date of disclosure. As such, Member States may adopt limitations to the rights and obligations provided for in this Directive. Any limitation must be a "*necessary, appropriate and proportionate measure within a democratic society on specific grounds of public policy, namely to safeguard national security (i.e. State security), defence and public security, or for the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of electronic communications systems*[353].

However, the CJEU subsequently invalidated this 2006 directive as contrary to the European Charter of Fundamental Rights with the 8 April 2014 ruling *Digital Rights Ireland* Ltd [354].

On 21 December 2016, the CJEU clarified the conditions of application of a generalized data retention obligation. In the *Tele2*[355] judgment, the Court considers that a generalized obligation to retain data, thus applying even to persons whom there is no reason to suspect of serious criminal offences, exceeds "*the limits of what is strictly necessary and cannot be regarded as being justified in a democratic society*".

More recently, the CJEU extended this reflection in the judgment of 6 October 2020[356] . The European judges considered that the obligation of general data retention by operators could only be provided for if it is:

- Temporarily limited to what is necessary
- Justified by a serious threat to national security that is actual, present or foreseeable
- Operated under the effective control of a judge or an independent administrative authority, whose decision has binding effect

The scope of these rulings has been interpreted differently in different Member States. The majority practice regarding the retention period obligation remains **1 year**, notably for France, Germany, Spain and the United Kingdom. Nevertheless, this obligation is discussed in the Netherlands since the case law of 2014, in a position favourable to the respect of privacy[357], while France, in a judgment of the Council of State dated 21 April 2021, considers that the generalized retention obligation is now justified by the existing threat to national security[358]. Furthermore, France wishes to maintain the

352 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, Article 6.

353 *Ibid,* recital 4.

354 CJEU, 8 April 2014, Digital Rights Ireland Ltd, Case C-293/12, [Online] Available : https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=221945

355 CJEU, 21 December 2016, *Tele2 Sverige AB*, Case. C-203/15, [Online] Available : https://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=FR

356 CJEU, 6 October 2020, joined cases C-511/18, C-512/18 and C-520/18, *op. cit.*

357 "Bewaarplicht telecomgegevens", Privacy Barometer, 13 March 2015. [Online] Available: https://www.privacybarometer.nl/maatregel/37/Bewaarplicht_telecomgegevens

358 Press release, "Connection data: the Council of State reconciles compliance with European Union law and the effectiveness of the fight against terrorism and crime", *Council of State*, Paris, 21 April 2021.

possibility of retaining such connection data to a greater extent than suggested by the Court of Justice, not wishing to comply with the conditions set out in the 2020 judgment[359].

In practice, the French Conseil d'État considered that compliance with these conditions (geographical and temporal limitation and limitation of the type of persons without discrimination) was technically impossible in criminal matters, since it would have been necessary to know in advance which person would be likely to commit a crime.

Other countries have shorter retention periods, and a further distinction can be made by the data collected, as the type of data retained by telecommunication operators and internet service providers varies from country to country.

However, the Court of Justice of the European Union has provided clarification in a recent ruling of 2 March 2021[360]. During a preliminary investigation, the public prosecutor or the judicial police officer may request the communication of personal location data from telephone operators. In this respect, the Court of Justice, when questioned by the Estonian Supreme Court, confronted the use of these personal data in criminal proceedings with the requirements of the Directive on the protection of privacy in the communications sector and the Charter of Fundamental Rights. Therefore, access to such data must be restricted to cases of serious crime or prevention of serious threats to public security and by exception in cases where "vital interests of national security, defence or public security are threatened by terrorist activities". In the 2021 judgment, the Court now requires prior control by a court or an independent authority of requests for access to personal data, including geolocation data, as they infringe on freedom of movement and privacy. Thus, the Court of Justice considered that the French public prosecutor's office did not have such independence: "This is not the case of a public prosecutor's office which directs the investigation procedure and exercises, where appropriate, public action. The task of the public prosecutor's office is not to decide a dispute independently, but to submit it, where appropriate, to the competent court, as a party to the proceedings bringing the criminal action".

5.4.3 Retention of other types of data

In November 2020, the Council of the European Union adopted a draft resolution that seeks to oblige operators of secure messaging systems such as WhatsApp or Signal to allow intelligence services to access content exchanged via privileged access. This initiative has so far remained unsuccessful.

5.4.4 Remarks on ePrivacy regulation and law enforcement

As noted above, the Law Enforcement Directive's material scope is limited to two cumulative conditions. The data processing must be carried out by the (i) competent authorities only for the (ii) purposes set forth on its article one. These purposes are "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"[361].

As for the competent authorities, in accordance with the definition made by the LED, they can be private entities, providing that they exercise public authority on a Member State's behalf.

---

359 JACQUIN Jean-Baptiste, "Le Conseil d'Etat autorise la conservation des données de connexion", *Le Monde*, 2021, [Online] Available: https://www.lemonde.fr/societe/article/2021/04/21/le-conseil-d-etat-autorise-la-poursuite-de-la-conservation-generalisee-des-donnees_6077560_3224.html

360 CJUE, 2 mars 2021, case C-746/18, [Online] Available: https://curia.europa.eu/juris/document/document.jsf?text=&docid=238381

361 Article 1 of the LED.

In other terms, if the providers of electronic communications services are not entrusted with public powers, the collection or storing of electronic evidence performed by them will not fall under the scope of LED, rather it will fall under the scope of the reformed ePrivacy regulation, which has not entered into force yet.

On the other hand, as per the ruling of the CJEU, if the LEAs access the electronic evidence retained by the providers of electronic communications, in this case this processing of data will fall under the scope of the ePrivacy directive[362]. CJEU argues that, in such a case, the access by the LEAs will concern the processing made by the providers of electronic communications services, which is regulated within the scope of the ePrivacy directive[363].

Hence, if the LEAs lawfully intercept telecommunications data themselves, this access will not fall into the scope of the ePrivacy directive, since the material scope of the ePrivacy directive excludes "activities of 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[364].

5.4.5 Perspectives and recommendations

A few years ago, European Commissioner Dimitris Avramopoulos stated that the European Commission did not intend to present a new proposal concerning the obligation to retain data for telecoms operators and internet providers[365]. As a result of this almost exclusively case law framework, it has been noted that the different interpretations by Member States of the case law of the CJEU lead to a fragmentation of practices regarding the collection and retention of connection data. One solution to this problem could be to harmonise the duration, conditions and types of data collected by the Member States.

In this respect, a report of April 2021 was drawn up by the association Le Club des juristes[366] , and raised in particular the issue of data retention by telecommunications operators. The working group proposed 10 recommendations to advance the fight against cybercrime. One of them proposed the adoption of a European data retention regime, which would aim to meet the operational needs of law enforcement and judicial authorities. This regime could provide for investigations to be carried out with data retained for up to one year.

Alongside a harmonisation of time limits, other related improvements could be made with regard to data retention. The establishment of a processing register and logging of accesses would make it possible to check the status of the collection of these data, and to verify the regularity of accesses to the databases. In order to maintain effectiveness in the fight against terrorism and the defence of national security, a staggered retention period could be introduced, allowing for a longer period when there are reasonable and objective suspicions about certain individuals at risk.

---

[362] CJEU, 21 December 2016, joined cases C203/15 and C698/15, *op. cit.,* §76 et seq.

[363] *Ibid*. §78.

[364] Regulation of the European Parliament and 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), 10 January 2017, [Online] Available : https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=EN

365 "Europa laat lidstaten zelf beslissen over bewaarplicht", Nu, 13 March 2015, [Online] Available : https://www.nu.nl/internet/4010268/europa-laat-lidstaten-zelf-beslissen-bewaarplicht.html

366 Le Club des juristes, "Le droit pénal à l'épreuve des cyberattaques", report of April 2021, p. 90.

Chapter 6 Summary and Conclusion

In conclusion, the use of encryption and its circumvention are not trivial from the angle of fundamental rights, to which the European Union and its member states are attached, legally and non-legally. The balance to be struck between these rights is reflected in the EXFILES project, which balances freedom of speech, the right to secrecy of correspondence, privacy, the right not to self-incriminate, and the security that States must guarantee through law enforcement.

Digital evidence has become almost unavoidable in criminal investigations, and its non-materiality also allows for more sharing of the data and information it generates; in order to respect the principles surrounding evidence that are guarantees of justice and the rule of law, special provisions are sometimes made by Member States regarding electronic evidence. However, this is not the case for all of them and this legal framework is rather dispersed, while information can circulate. Positive law of evidence applies to electronic evidence, which is therefore regulated, but the particularities of investigations in the digital world are not sufficiently taken into account by the law, leaving uncertainties. Supranational instruments, particularly from the Council of Europe, but also from the European Union, promote and facilitate exchanges, sometimes to the detriment of fundamental rights in this fragile and dispersed legal framework.

The protection of personal data, both content and metadata, is a major issue for individuals, law enforcement agencies and service providers alike. Thus, many legal issues surround the cooperation between the two latter, which is conflicting, sometimes technically complicated, and suffers from an insufficient, disparate and often inoperative legal framework. Recommendations on this point will still have to be formulated, but the EU legal framework is evolving positively on this crucial point.

In order to improve legal certainty for all stakeholders, trust in institutions, the use of secure technology, and the effectiveness of justice, the framework for the exploitation of electronic evidence through collection, preservation, exchange and finally the production in courts of law will have to be further improved and harmonised in line with the fundamental principles of the Union. The chain of custody and admissibility of evidence in court in the EU will be analysed in the deliverable 2.3 of this project.

Chapter 7 List of Abbreviations

Abbreviation	Translation
BKA	Bundeskriminalamt (German Federal Criminal Police Office)
BKAG	Gesetz über das Bundeskriminalamt (Law on the German Federal Criminal Police Office)
CCF	Commission for the Control of Interpol's Files
CDPC	European Committee on Crime Problems
CERT	Computer Emergency Response Team
CETS N°223	Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 18 May 2018
CJEU	Court of Justice of the European Union
CNCTR	Commission nationale de contrôle des techniques de renseignement (French National Commission for the Control of Intelligence Techniques)
CNIL	Commission Nationale Informatique et Libertés (French data protection authority)
Convention 108+	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS N°108)
CoSSeN	Commandement spécialisé pour la sécurité nucléaire (French Specialised Command for Nuclear Security)
CPCE	Code des postes et des communications électroniques (French post and electronic communications code)
C-PROC	Cybercrime Programme Office of the Council of Europe
CRPA	Code des relations entre le public et l'administration (French Code of relationships between the public and the administration)
CSIRT	Computer Security Incident Response Team
DNA	Deoxyribonucleic acid
DPO	Datat protection officer
E2EE	End-to-end encryption
EC	European Commission
ECHR	European Court of Humain Rights
E-CODEX System	e-Justice Communication via Online Data Exchange
EConv.HR	European Convention of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
eEDES	e-Evidence Digital Exchange System
eIDAS	Electronic IDentification Authentication and trust Services
EIO	European Investigation Order
EIS	Europol Information System
ENISA	European Union Agency for Cybersecurity
EPE	Europol Expert Group
ESMA	European Securities and Markets Authority
EU	European Union

Abbreviation	Translation
EU-LISA	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
EWCA	England and Wales Court of Appeal
Fead	Fichier automatisé des empreintes digitales (French Automated Fingerprint File)
FIC	Forum international de la cybersécurité
FIJAUS	Fichier judiciaire automatisé des auteurs d'infractions sexuelles ou violente (French List of perpetrators of sexual or violent offenses)
Fnaeg	Fichier national automatisé des empreintes génétiques (French Automated National DNA File)
GCHQ	Government Communications Headquarters of United Kingdom
GDPR	General Data Protection Regulation
HR	Hoge Raad der Nederlanden (Supreme Court of the Netherlands)
ICCPR	United Nations International Covenant on Civil and Political Rights
ICO	Information Commissioner's Office of United Kingdom
IMEI	International Mobile Equipment Identity
Interpol	International Criminal Police Organization
IOSCO	International Organization of Securities Commissions
IP	Internet Protocol
IPA	United Kingdom Investigatory Powers Act 2016
IPC	Intellectual Property Code
IPT	Investigatory Powers Tribunal of United Kingdom
IRCGN	Institut de recherche criminelle de la Gendarmerie nationale (French National Gendarmerie Criminal Research Institute)
JHA	Justice and Home Affairs
LCEN	French Law no. 2004-575 For Confidence in the Digital Economy of 21 June 2004
LEAs	Law Enforcement Agencies
LECrim	Ley de Enjuiciamiento Criminal (Spanish Code of Criminal Procedure)
LED	Law Enforcement Directive (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)
LIL	Loi Informatique et Libertés (French Data Protection Act)
Loi SILT	Loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (French Law on Internal security and the fight against terrorism)
LOPPSI 2	Loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (French Law on the orientation and programming for the performance of internal security)

Abbreviation	Translation
LRPDJ	Logiciel de rédaction des procédures de la douane judiciaire (French Customs procedure drafting software)
LRPGN	Logiciel de rédaction des procédures de la gendarmerie nationale (French Software for writing national gendarmerie procedure)
LRPPN	Logiciel de rédaction des procédures de la police nationale (French National Police Procedures Writing Software)
MAC	Media Access Control
MI5	Military Intelligence, Section 5 (Security Service of United Kingdom)
MI6	Secret Intelligence Service
MLAT	Mutual legal assistance treaties
N.SIS	Uniform national interface
NCA	National Crime Agency
NFI	Netherlands Forensic Institute
NGO	Non-governmental organization
OHCHR	United Nations Office of the High Commissioner on Human Rights
OJFR	Official Journal of French Republic
PC-CY	Committee of Experts on Crime in Cyberspace of the Council of Europe
PJGN	Pôle judiciaire de la Gendarmerie nationale (French Judicial Department of the National Gendarmerie)
QPC	Priority question of constitutionality
SCRC	French Gendarmerie Nationale's Central Criminal Intelligence Service
SCRCGN	Service Central de Renseignement Criminel de la Gendarmerie Nationale (French Criminal intelligence central office)
SIM	Subscriber Identity Module
SIS II	Second generation Schengen Information System
SMS	Short Message Service
SNEAS	National Service for Administrative Security Investigations
TAC	Technical Assistance Centre
TAJ	Traitement des antécédents judiciaires (French Criminal record file)
TCN	Technical capability notice
T-CY	Cybercrime Convention Committee
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom
UN	United Nations
UNDOC	United Nations Office on Drugs and Crime
US	United States (of America)
WPG	Dutch Police Data Act

Chapter 8 Bibliography

I. Texts

i. International and European Texts

United Nations, *Charter of the United Nations*, 26 June 1945.

United Nations, *United Nations Universal Declaration of Human Rights*, 10 December 1948.

Council of Europe, *European Convention of Human Rights* (EConv.HR), 4 November 1950.

INTERPOL Office of legal affairs, *Constitution of the International Criminal Police Organization*, 1956.

Council of Europe, *European Convention on Mutual Assistance in Criminal Matters*, 20 April 1959.

United Nation Office of the High Commissioner on Human Rights (OHCHR), *International Covenant on Civil and Political Rights*, 16 December 1966.

Council of Europe, *Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, 17 March 1978.

Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 28 January 1981.

United Nations, *United Nations Convention against Transnational Organized Crime*, New York, 15 November 2000.

Council of Europe, *Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, 8 November 2001.

Council of Europe, *Explanatory Report to the Convention on Cybercrime*, 23 November 2001.

Council of Europe, Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, as adopted by the Committee of Ministers on 17 November 2021.

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*

Council of the European Union, *Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.*

Council of the European Union, *Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime*.

European Parliament and Council, *Proposal for a Regulation of the European Parliament and of the Council on European orders for the production and preservation of electronic evidence in criminal matters,* 17 April 2018.

European Parliament and Council, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters,* 17 April 2018.

European Parliament and Council, *Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA*, 11 May 2016.

European Parliament and Council*, Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II),* 20 December 2006.

European Parliament and Council, *Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU,* 28 November 2018.

European Parliament and Council, *Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006*, 28 November 2018.

European Parliament and Council, *Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals,* 28 November 2018.

European Parliament and Council, *Proposal for a Regulation of the European Parliament and of the Council on a computerised system for communication in cross-border civil and criminal proceedings (e-CODEX system), and amending Regulation (EU) 2018/1726*, 2 December 2020.

List of competent authorities which are authorised to search directly the data contained in the second generation Schengen Information System pursuant to Article 31(8) of Regulation (EC) No 1987/2006 of the European Parliament and of the Council and Article 46(8) of Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System, *OJ C 278, 22.8.2014, p. 1–144.*

United Nations Office on Drugs and Crime (UNODC), *United Nations Convention Against Transnational Organized Crime and the Protocols Thereto*, New-York, 2004.

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.

Council of Europe, Committee on Political Affairs and Democracy of the Parliament Assembly, *Establishment of a "Partner for Democracy" Status with the Parliamentary Assembly*, 14 May 2009.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Regulation of the European Parliament and 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), 10 January 2017.

Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 strengthening certain aspects of the presumption of innocence and the right to be present at trial in criminal proceedings.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

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 (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.

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.

European Parliament and Council, "Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters", 17 April 2018.

Council of Europe, *Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 10 October 2018.

Council of Europe, Cybercrime Convention Committee, *Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime*, 23 June 2019.

Council of Europe, Cybercrime Convention Committee, *Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime. Provisional Text*, 2020.

INTERPOL, « Règlement d'INTERPOL sur le traitement des données », [III/IRPD/GA/2011 (2019)].

ii. National texts

FRANCE

Decree no. 2016-67 of 29 January 2016 on intelligence gathering techniques.

Decrees no. 2021-1361 and 2021-1363 of 20 October 202.

French Civil Code.

French Code of Criminal Procedure.

French Code of Relations Between the Public and the Administration.

French Postal and Electronic Communications Code.

French Code of Internal Security.

French Code of Intelligence, no. 2015-912 of 24 July 2015.

Law no 2011-267 of 14 March 2011 on the orientation and programming for the performance of internal security.

Law no. 2021-998 of the 30 July 2021 on the prevention of terrorist acts and intelligence.

Law no. 2018/493 of 20 June 2018 on the protection of personal data.

Law no. 78-17 of 6 January 1978 on information technology, data files and civil liberties.

Law no. 2004-575 of 21 June 2004 for Confidence in the Digital Economy.

GERMANY

German Code of Criminal Procedure

Law on the more effective and practicable organisation of criminal proceedings of 17 August 2017, Bundesgesetzblatt 2017 Part I no 58 of 23 August 2017, page 3202.

Ordinance on the Technical and Organisational Implementation of Telecommunications Surveillance Measures "Telekommunikations-Überwachungsverordnung - TKÜV".

NETHERLANDS

Dutch Code of Criminal Procedure

Intelligence and Security Services Act 2017 "Wet op de inlichtingen- en veiligheidsdiensten 2017",

Police Data Act: the Wet Politiegegevens (WPG)

Telecommunications Act "*Telecommunicatiewet*

SPAIN

Spanish Code of Criminal Procedure

Spanish Law on Data Protection

Organic Law 13/2015 amending the Criminal Procedure Law for the strengthening of procedural guarantees and the regulation of technological investigation measures, 5 October 2015.

Organic Law 7/2021, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and the execution of criminal sanctions, 26 May 2021.

UK

Police and Criminal Evidence Act 1984.

Investogatory Powers Act 2016

NORWAY

Norwegian Code of Criminal Procedure

Intelligence Services Act "*etterretningstjenesteloven*", 19 June 2020

II. Reports

Article 29 Data Protection Working Party, “Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive”, 26 February 2013.

Contribution of the EDPB to the European Commission’s evaluation of the Data Protection Law Enforcement Directive (LED) under Article 62, adopted on 14 December 2021.

General interministerial instruction on the protection of secrecy and information concerning national defence and State security no. 1300/SGDN/ PSE/SSD of 25 August 2003. [Online] Available : [https://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/instruction-generale-interministerielle-n-1300-sur-la-protection-du-secret-de-la-defense-nationale/].

European Commission, "Memo on the Green Paper on Detection and Associated Technologies in the Work of Law Enforcement, Customs and Other Security Authorities", 4 September 2006, p. 3 [Online] Available: [https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_06_317/MEMO_06_317_EN.pdf].

European Commission, Directorate-General for Migration and Home Affairs, Dupont, C., Cilli, V., Omersa, E., et al., *Study on the retention of electronic communications non-content data for law enforcement purposes: final report*, Publications Office, 2020. [Online] Available: [https://data.europa.eu/doi/10.2837/384802].

European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on a computerised system for communication in cross-border civil and criminal proceedings (e-CODEX system), and amending Regulation (EU) 2018/1726 (COM(2020)0712 – C9-0389/2020 – 2020/0345(COD)), 15 October 2021. [Online] Available: [https://www.europarl.europa.eu/doceo/document/A-9-2021-0288_EN.pdf].

French Conseil d’État, Report on "Le droit souple", 2013 Annual study n° 64, 2013. [Online] Available: [https://www.vie-publique.fr/sites/default/files/rapport/pdf/144000280.pdf].

United Nations Office on Drugs and Crime (UNODC), "Comprehensive Study on Cybercrime", *United Nations Office on Drugs and Crime*, February 2013, p. 158 [Online] Available: [https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf].

French Ministry of Interior, "Answer of the French Ministry of Interior to the written question n°10778", published in the Official Journal of French Republic (*OJFR*) on 18 February 2020, p. 1259. [Online] Available: [https://questions.assemblee-nationale.fr/q15/15-10778QE.htm].

INTERPOL, *Global Cybercrime Strategy - Summary*, 2016 [Online] Available: [https://www.interpol.int/en/content/download/5586/file/Summary_CYBER_Strategy_2017_01_EN%20LR.pdf].

Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Prossessing of Personal Data, and Directorate General of Human Rights and Rule of Law, "Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data", 23 January 2017 [Online] Available: [https://rm.coe.int/t-pd-2017-1-bigdataguidelines-en/16806f06d0].

Council of the European Union, Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime", 2 October 2017 [Online] Available: [https://data.consilium.europa.eu/doc/document/ST-12711-2017-INIT/en/pdf].

Koops Commission Report, 'Regulering van opsporingsbevoegdheden in een digitale omgeving', 2018. [Online] Available: [https://www.njb.nl/umbraco/uploads/2019/3/Rapport-Commissie-Koops-juni-2018.pdf].

Council of Europe, Directorate General of Human Rights and Rule of Law, and Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Prossessing of Personal Data, "Guidelines on Artificial Intelligence and Data Protection", 25 January 2019 [Online] Available: [https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8].

Council of Europe, Directorate General of Human Rights and Rule of Law and Cybercrime Division, "Electronic Evidence Guide, a Basic Guide for Police Officers, Prosecutors and Judges", 2020, pp. 11-13 [Online] Available: [https://rm.coe.int/c-proc-electronic-evidence-guide-2-1-en-june-2020-web3/16809efd7f].

Council of European Union, "Security through encryption and security despite encryption", 24 November 2020. [Online] Available [https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf].

Council of Europe, "Explanatory report to the Second Additional Protocol as noted by the Committee of Ministers on 17 November 2021", 17 November 2021 [Online] Available: [https://rm.coe.int/1680a49c9d].

Council of Europe, Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, 17 November 2021, p. 14. [Online] Available: [https://rm.coe.int/1680a49c9d].

FRAYSSINET (J.), « Interpol et ses fichiers », 2017, p.3, [Online] Available: https://hal.archives-ouvertes.fr/hal-01427564

ICO, “Mobile phone data extraction by police forces in England and Wales”, June 2020, p. 45, [Online] Available : https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/

Le Club des juristes, "Le droit pénal à l'épreuve des cyberattaques", report of April 2021, p. 90.

III. Case Law

ECHR, 23 July 1968, no 1474/62 Case “relating to certain aspects of the laws on the use of languages in education in Belgium” v. Belgium.

ECHR, 7 December 1976, no 5493/72, *Handyside v The United Kingdom*.

ECHR, 6 September 1978, no 5029/71, *Klass and others v. Germany*.

ECHR, , 11 March 1987, no. 10964/84, Brozicek c. Italie.

ECHR, 24 April 1990, no 11801/85, *Krusslin v. France*.

ECHR, 25 February 1993, no 10828/84, *Funke v France*.

ECHR, 8 February 1996, no. 18731/91, *John Murray v. the United Kingdom*.

ECHR, 17 December 1996, no 19187/91, *Saunders v. United Kingdom*.

ECHR, 25 June 1997, no 20605/92, *Halford v. United Kingdom*.

ECHR, 25 July 2000, no. 23969/94, *Mattoccia c. Italie*.

ECHR, 21 December 2000, no. 34720/97, *McGuinness v. Ireland*.

ECHR, 1 July 1961, no.332/57, *Lawless v. Ireland*

ECHR, 8 December 2008, no.30562/04 and 30566/04*, S. and MARPER v. United Kingdom*

Spanish Constitutionnel Tribunal, 1st Chamber, 22 April 2002, Sentencia 83/2002.

ECHR, 5 November 2002, no. 48539/99, *Allan v. United Kingdom*.

ECHR, 27 September 2005, no 50882/99, *Petri Sallinen and others v. Finland*.

French Cour de cassation, Criminal chamber, 11 May 2006, nº 05-84.837.

ECHR, 11 July 2006, no. 54810/00, *Jalloh v. Germany*.

ECHR, 29 June 2007, nos. 15809/02 and 25624/02, O'Halloran and Francis v. the United Kingdom.

ECHR, 22 May 2008, no 65755/01, *Iliya Stefanov v. Bulgaria*.

ECHR, 14 October 2010, no. 1466/07, *Brusco v. France*.

ECHR, 6 December 2012, *Michaud v. France*.

ECHR, 22 June 2017, no. 8806/12, *Aycaguer v. France*

Supreme Court of the United States, 25 June 2014, *Riley v. California*, 134 S.Ct. 2473, 2493.

Spanish Suprem Tribunal, 19 May 2015, STS 2047/2015.

Spanish Suprem Tribunal, Criminal chamber, 4 December 2015, STS 786/2015.

ECHR**,** 4 December 2015, no 47143/06, *Roman Zakharov v. Russia*.

Dutch Rechtbank Amsterdam, 20 July 2017, no. 13/997096-15.

French Constitutional Court, decision no. 2018-696 QPC of 30 March 2018.

French Constitutional Court, decision no. 2017-670 QPC of 27 October 2017

French Constitutional Court, decision no. 2010-25 QPC of 16 September 2010.

French Council of State, decision no. 360759 of 11 April 2014

French Cour de cassation, Criminal chamber, 10 December 2019, no. 18-86.878.

ECRH, 14 January 2020, no. 35989/14, *Stephens v. Malta*.

CJEU, 6 October 2020, Case C-623/17, *Privacy International*, and in Joined Cases C-511/18, *La Quadrature du Net and Others*, C-512/18, *French Data Network and Others*, and C-520/18, *Ordre des barreaux francophones et germanophone and Others*.

CJEU, 16 July 2020, Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*

CJEU, 21 December 2016, joined cases C203/15 and C698/15, *Tele2 Sverige AB vs. Post- och telestyrelsen and Secretary of State for the Home Department contre Tom Watson e.a.*

CJEU, 8 April 2014, Case C-293/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a.*

CJEU, 2 March 2021, Case C-746/18, *H.K./Prokuratuur.*

Dutch Parket bij de Hoge Raad, 13 October 2020, ECLI:NL:PHR:2020:927.

ECHR, 27 October 2020, nos. 1191/08 and 29084/07, *Ayetullah Ay c. Turquie*.

ECHR, 1 December 2020, no. 46712/15, *Berkman v. Russia*.

French Cour de cassation, Criminal chamber, 12 January 2021, no. 20-84045.

Dutch Hoge Raad, 9 February 2021, ECLI:NL:HR:2021:202.

ECHR, 25 May 2021, no 35252/08, *Centrum för Rättvisa v. Sweden*.

ECHR, 25 May 2021, nos 58170/13, 62322/14 and 24960/151, *Big Brother Watch and Others v. United Kingdom*.

England and Wales Court of Appeal (Criminal Division), 5 February 2021, A, B, D, & C v. Regina.

Rechtbank Rotterdam, 22 February 2019, no. 10/960268-18. [Online] Available: [https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBROT:2019:2712].

IV. Literature

The Collection of Electronic Evidence in Germany: A Spotlight on Recent Legal Developments and Court Rulings [Online] Available: https://link.springer.com/chapter/10.1007%2F978-981-10-5038-1_1

V. Reviews

Bismuth R., « Le Cloud Act face au projet européen e-evidence », *Revue critique de droit international privé*, 2019, p. 1.

L. Dargent, 'Council of Europe: guidelines on electronic evidence in civil and administrative proceedings', Dalloz Actualité, 12 February 2019.

O. Haddad, "Garde à vue: ne dites rien, votre téléphone parlera pour vous", *Dalloz Actualité*, 7 April 2021.

M-C. Montecler, "La CEDH admet le principe de la surveillance électronique de masse", *Dalloz Actualité*, 28 May 2021.

VI. Press articles

FOLLOROU Jacques, UNTERSINGER Martin,"Le réseau crypté EncroChat infiltré par les polices européennes : " C'est comme si nous étions à la table des criminels "', *Le monde*, 3 July 2020. [Online] Available: [https://www.lemonde.fr/international/article/2020/07/03/c-est-comme-si-nous-etions-a-la-table-des-criminels-comment-les-polices-europeennes-ont-penetre-le-reseau-crypte-encrochat_6045024_3210.html].

JACQUIN Jean-Baptiste, "Le Conseil d'Etat autorise la conservation des données de connexion", *Le Monde*, 2021, [Online] Available: https://www.lemonde.fr/societe/article/2021/04/21/le-conseil-d-etat-autorise-la-poursuite-de-la-conservation-generalisee-des-donnees_6077560_3224.html

"Zweeds hof verwerpt EncroChat-bewijs," *Crimesite*, 12 May 2021. [Online] Available: [https://www.crimesite.nl/zweeds-hof-verwerpt-encrochat-bewijs/].

Press release, "Connection data: the Council of State reconciles compliance with European Union law and the effectiveness of the fight against terrorism and crime", *Council of State*, Paris, 21 April 2021.

VII. Websites

ATTARD Isabelle, National Assembly, Discussion of the Intelligence Bill, 14 April 2015, [Online] Available : https://www.assemblee-nationale.fr/14/cri/2014-2015/20150215.asp

"Bewaarplicht telecomgegevens", Privacy Barometer, 13 March 2015. [Online] Available: https://www.privacybarometer.nl/maatregel/37/Bewaarplicht_telecomgegevens

CJEU, press release No. 22/21 of the 25 February 2021. [Online] Available: [https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-02/cp210022fr.pdf

CNIL, « Comment déterminer la notion d'interconnexion ? » [online] Available: https://www.cnil.fr/en/node/15316 [consulté le 06/01/2021].

CNIL, deliberation no. 2011-204 of 7 July 2011. [Online] Available : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000025804888

CNIL, deliberation no. SAN-2021-016 of 24 September 2021. [Online] Available : https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044115170

Commission for the control of INTERPOL's files (CCF), [Online] Available: https://www.interpol.int/fr/Qui-nous-sommes/Commission-de-controle-des-fichiers-d-INTERPOL-CCF

De Gaulle Fleurance and Associates, « The Court of Justice of the European Union sets limits to mass surveillance », 27 October 2020, [Online] Available : https://www.degaullefleurance.com/en/the-court-of-justice-of-the-european-union-sets-limits-to-mass-surveillance/#_ftn1 [Accessed 5 January 2022].

"Denmark: geolocation at the origin of thousands of judicial errors?", Le Point, 24 August 2019. [Online] Available: [https://www.lepoint.fr/high-tech-internet/danemark-la-geolocalisation-a-l-origine-de-milliers-d-erreurs-judiciaires-24-08-2019-2331426_47.php].

"Encrochat: juridisch kader onderzoekswensen", *Weening Strafrechtadvocaten*, 27 January 2021, p. 7. [Online] Available: [https://www.strafrechtadvocaten.nl/encrochat-juridisch-kader-onderzoekswensen/].

"Encrochat Hack: Can Illegally Obtained Evidence Be Used Against You?", Ashmans Solicitors, 17 July 2020. [Online] Available : [https://www.ashmanssolicitors.com/articles/encrochat-hack-can-illegally-obtained-evidence-be-used-against-you/].

The French Council of State, « Opinion on a draft law adapting Law No. 78-17 of 6 January 1978 on information technology, files and freedoms to European Union law», 7 December 2017, [Online] Available: https://www.conseil-etat.fr/ressources/avis-aux-pouvoirs-publics/derniers-avis-

publies/adaptation-au-droit-de-l-union-europeenne-de-la-loi-n-78-17-du-6-janvier-1978-relative-a-l-informatique-aux-fichiers-et-aux-libertes

"Improving Cross-Border Access to Electronic Evidence", *System Upgrade*, January 2019 [Online] Available: [https://www.gppi.net/media/GPPi_2018_Hohmann_Barnett_System_Upgrade.pdf].

D. W. Bennett, "The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations", *Forensic Focus*, 22 August 2011 [Online] Available: [https://www.forensicfocus.com/articles/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/].

P. Beuth & K. Biermann, "Dein trojanischer Freund und Helfer", *Zeit Online*, 22 June 2017. [Online] Available: [https://www.zeit.de/digital/datenschutz/2017-06/staatstrojaner-gesetz-bundestag-beschluss/komplettansicht].

Pôle judiciaire de la gendarmerie nationale IRCGN - SCRCGN, « Geolocation data analysis with GendExif », [Online] Available : https://www.gendarmerie.interieur.gouv.fr/pjgn/innovation/les-brevets-et-innovations/l-analyse-de-donnees-de-geolocalisation-avec-gendexif

Council of Europe, "Our Member States", [Online] Available: [https://www.coe.int/en/web/about-us/our-member-states].

Council of Europe - Cybercrime, "Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY", [Online] Available: [https://www.coe.int/en/web/cybercrime/parties-observers].

Council of Europe - Data Protection, "Convention 108+ : The Modernised Version of a Landmark Instrument", 18 May 2018 [Online] Available: [https://www.coe.int/en/web/data-protection/newsroom/-/asset_publisher/7oll6Oj8pbV8/content/modernisation-of-convention-108].

Council of Europe, *Convention 108+ Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, June 2018 [Online] Available: [https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1].

Council of Europe, 'Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings', CM(2018)169-add1final, 30 January 2019. [Online] Available : [https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902dc9].

Council of Europe, Cybercrime Convention Committee, "The Budapest Convention on Cybercrime: Benefits and Impacts in Practice", 13 July 2020, p. 5 [Online] Available: [https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac].

Council of the EU press release, "Encryption: Council adopts resolution on 'Security through encryption and despite encryption'", 14 December 2020. [Online] Available: [https://www.consilium.europa.eu/fr/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/].

European Data Protection Supervisor (EDPS), "Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit", 2017 [Online] Available: [https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_fr.pdf].

EDPS, "EDPS Opinion on Proposals Regarding European Production and Preservation Orders for Electronic Evidence in Criminal Matters", 2019 [Online] Available: [https://edps.europa.eu/sites/edp/files/publication/19-11-06_opinion_on_e_evidence_proposals_fr.pdf].

European project on Evidence, "European Informatics Data Exchange Framework for Courts and Evidence", *Cordis*. [Online] Available: [https://cordis.europa.eu/project/id/608185].

European Union Agency for Cybersecurity (ENISA), "On the free use of cryptographic tools for (self) protection of EU citizens", 20 January 2016. [Online] Available: [https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-position-on-crypto].

European Commission, « Modernising EU justice systems - Questions and Answers », 2 December 2020. [Online] Available: [https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2247].

European Commission, "Security Union: Commission facilitates access to electronic evidence". [Online] Available: [https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3343].

European Council, « Digitalisation of justice: Council presidency and European Parliament reach provisional agreement on e-CODEX », 8 December 2021. [Online] Available: [https://www.consilium.europa.eu/en/press/press-releases/2021/12/08/digitalisation-of-justice-council-presidency-and-european-parliament-reach-provisional-agreement-on-e-codex/].

Eurojust, "The Encrochat investigation in France", 2 July 2020. [Online] Available: [https://www.eurojust.europa.eu/sites/default/files/Press/2020-07-02_EncroChat-investigation-in-France_FR.pdf].

ENISA, "Cooperation between CSIRTs and Law Enforcement: Interaction with the Judiciary", *ENISA*, November 2018 [Online] Available: [https://www.enisa.europa.eu/publications/csirts-le-cooperation].

"Encrochat: juridisch kader onderzoekswensen", *Weening Strafrechtadvocaten*, 27 January 2021, p. 24. [Online] Available: [https://www.strafrechtadvocaten.nl/encrochat-juridisch-kader-onderzoekswensen/].

EU-Lisa, [Online] Available: https://www.eulisa.europa.eu/

EU-LISA, "SIS The most widely used IT system for security and border management in Europe" [Online] Available: https://www.eulisa.europa.eu/Publications/Information%20Material/Leaflet%20SIS.pdf

EUROPOL, *SIRIUS EU Digital Evidence Situation Report*, 2ndAnnual Report, 2020, [Online] Available: https://www.europol.europa.eu/cms/sites/default/files/documents/sirius_desr_2020.pdf

Europol platform for experts, [Online] Available: https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-platform-for-experts

EUROPOL, « Europol launches the SIRIUS platform to facilitate online investigations », 31 October 2017, [Online] Available : https://www.europol.europa.eu/media-press/newsroom/news/europol-launches-sirius-platform-to-facilitate-online-investigations

"Europa laat lidstaten zelf beslissen over bewaarplicht", Nu, 13 March 2015, [Online] Available : https://www.nu.nl/internet/4010268/europa-laat-lidstaten-zelf-beslissen-bewaarplicht.html

EDPB, Schengen Information System II Supervision Coordination Group (SIS II SCG), [Online] Available: https://edps.europa.eu/data-protection/european-it-systems/schengen-information-system_fr

Forum international de la cybersécurité (FIC), "EncroChat: Deciphering of the End-to-End Encryption Service Used by Criminals - International Cybersecurity Observatory", *Observatoire du FIC*, 15 July 2020. [Online] Available: [https://observatoire-fic.com/en/encrochat-deciphering-of-the-end-to-end-encryption-service-used-by-criminals/].

Ho-Dac M., « European Parliament Report on the Proposal for a Regulation on e-CODEX System », 19 October 2021. [Online] Available: [https://eapil.org/2021/10/19/european-parliament-report-on-the-proposal-for-a-regulation-on-e-codex-system/].

Legal and administrative information directorate, "Automated National DNA File (Fnaeg)", [Online] Available: [https://www.service-public.fr/particuliers/vosdroits/F34834]. [Accessed 12 janvier 2022]

Legal and administrative information directorate, "Automated Fingerprint File (Faed)", [Online] Available: [https://www.service-public.fr/particuliers/vosdroits/F34835]. [Accessed 12 janvier 2022]

V. Garcia, "Le Royaume-Uni instaure la surveillance de masse de sa population", *L'express*, 30 November 2016. [Online] Available: [https://lexpansion.lexpress.fr/high-tech/le-royaume-uni-instaure-la-surveillance-de-masse-de-sa-population_1855595.html].

T. Heckermann, "Droit de l'espace numérique", FIC, 15 March 2021. [Online] Available : [https://observatoire-fic.com/droit-de-lespace-numerique/].

INTERPOL, "INTERPOL and the United Nations", [Online] Available: [https://www.interpol.int/en/Our-partners/International-organization-partners/INTERPOL-and-the-United-Nations].

INTERPOL, "Today's Priorities for UN-INTERPOL Collaboration", [Online] Available: [https://www.interpol.int/en/Our-partners/International-organization-partners/INTERPOL-and-the-United-Nations/Today-s-priorities-for-INTERPOL-United-Nations-collaboration].

INTERPOL, "Data Protection", [Online] Available: [https://www.interpol.int/en/Who-we-are/Legal-framework/Data-protection].

INTERPOL, "Commission for the Control of INTERPOL's Files (CCF)", [Online] Available: [https://www.interpol.int/en/Who-we-are/Commission-for-the-Control-of-INTERPOL-s-Files-CCF].

MoxieO, "Exploiting vulnerabilities in Cellebrite UFED and Physical Analyzer from an app's perspective", Signal, 21 April 2021. [Online] Available : [https://signal.org/blog/cellebrite-vulnerabilities/].

Observatoire des libertés et du Numérique, "Positioning of the Observatoire des libertés et du Numérique on Encryption, security and freedoms", *Ligue des droits de l'homme*, 12 January 2017, p. 6. [Online] Available: [https://www.ldh-france.org/wp-content/uploads/2017/01/201701.OLN_.Chiffrementsecuritelibertes.pdf].

R. Pfefferkorn, "I have a lot to say about Signal's Cellebrite hack", Stanford Law School Blog, 12 May 2021. [Online] Available : [https://cyberlaw.stanford.edu/blog/2021/05/i-have-lot-say-about-signal%E2%80%99s-cellebrite-hack].

Riehle C., « 2019 Counter-Terrorism Report by Eurojust », 12 February 2021. [Online] Available: [https://eucrim.eu/news/2019-counter-terrorism-report-by-eurojust/].

M. Rees, « Renseignement : trois boîtes noires, moins de 10 personnes à risque identifiées en France », *Nextinpact*, 23 August 2019. [Online] Available: [https://www.nextinpact.com/article/29611/108145-renseignement-trois-boites-noires-moins-10-personnes-a-risque-identifiees-en-france].

S. O'Dea, "Number of smartphone users worldwide from 2016 to 2023", *Statista*, 31 March 2021. [Online] Available : [https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/].

QUEZADA Katherine, "Highlights of the Spanish Act on Data Protection in the Area of Police and Criminal Justice (Organic Law 7/2021)", 15 juin 2021. [Online] Available: [https://www.law.kuleuven.be/citip/blog/highlights-of-the-spanish-act-on-data-protection-in-the-area-of-police-and-criminal-justice/].

SIRIUS, Section « Adhésion et accès » [Online] Available : https://www.eurojust.europa.eu/sirius

SIRIUS Project, SIRIUS Cross-Border Access to Electronic Evidence, [Online] Available: https://www.europol.europa.eu/operations-services-and-innovation/sirius-project

THIERRY Gabriel, "l'infiltration des smartphones Encrochat décapite la criminalité européenne'', *Lessor*, 25 June 2021. [Online] Available: [https://lessor.org/societe/linfiltration-des-smartphones-encrochat-decapite-la-criminalite-europeenne/].

Wahl T., *Infringement Proceedings for Not Having Transposed EU Data Protection Directive*, 10 September 2018. [Online] Available: [https://eucrim.eu/news/infringement-proceedings-not-having-transposed-eu-data-protection-directive/].

WILSON Alexandra, "Alexandra Wilson examines the Court of Appeal 'Encrochat' judgment: A, B, D & C v Regina [2021] EWCA Crim 128", *5SAH,* 25 March 2021. [Online] Available: [https://www.5sah.co.uk/knowledge-hub/articles/2021-03-25/alexandra-wilson-examines-the-court-of-appeal-encrochat-judgment-a-b-d-and-c-v-regina-2021-ewca-crim-128].