Benjamin Flander, Anže Erbežnik

TOOLKIT FOR HANDLING AND ADMISSIBILITY OF ELECTRONIC EVIDENCE

EMPOWERING LEGAL PRACTITIONERS TO CRITICALLY REVIEW ELECTRONIC EVIDENCE FROM THE PROCEDURAL RIGHTS PERSPECTIVE

Benjamin Flander, Anže Erbežnik

TOOLKIT FOR HANDLING AND ADMISSIBILITY OF ELECTRONIC EVIDENCE

EMPOWERING LEGAL PRACTITIONERS TO CRITICALLY REVIEW ELECTRONIC EVIDENCE FROM THE PROCEDURAL RIGHTS PERSPECTIVE

Funded by the European Union

This deliverable was funded by the European Union under Grant Agreement 101056685. The content of this report, including views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the European Commission can be held responsible for them.

ANNALES ZRS

Koper, 2024

TOOLKIT FOR HANDLING AND ADMISSIBILITY OF ELECTRONIC EVIDENCE
Empowering Legal Practitioners to Critically Review E-Evidence from the Procedural Rights Perspective

This book is a deliverable of the INNOCENT - Improving the application of the presumption of innocence when applying electronic evidence, funded by the European Commission (JUST) and coordinated by the Law and Internet Foundation, Bulgaria.

Authors: **Benjamin Flander, Anže Erbežnik**

Review: Dr Marin Bonačić, Dr Sabina Zgaga Markelj

Editor-in-Chief of Annales ZRS: Tilen Glavina

Technical editors: Alenka Obid, Barbara Pandev

Design and layout: Alenka Obid

Proofreading: Taia INT d.o.o.

Publisher: Znanstveno-raziskovalno središče Koper, Annales ZRS / Science and Research Centre Koper, Annales ZRS

For the publisher: Rado Pišot

Koper, 2024

Online edition, available at: https://doi.org/10.35469/978-961-7195-42-2

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani
COBISS.SI-ID 194189315
ISBN 978-961-7195-42-2 (PDF)

CONTENTS

EXECUTIVE SUMMARY

This Toolkit was created by the Law Institute of the Science and Research Centre of Koper, Slovenia, as a deliverable of the Innocent project. It is funded by the European Commission under the JUST Programme and coordinated by the Law and Internet Foundation, Bulgaria. It aims to enhance the application of the presumption of innocence when handling electronic evidence (e-evidence) in criminal proceedings and empower legal practitioners to critically review e-evidence from a procedural rights perspective. It is designed to enhance understanding of the legal and practical challenges encountered by judges, prosecutors and defence lawyers (particularly those operating in Central and Eastern Europe) in the acquisition of e-evidence by law enforcement agencies, evaluation of admissibility of e-evidence by judges, and cross-border access to and exchange of e-evidence.

Exploring the different stages in the life cycle of e-evidence, this Toolkit concerns data and evidence stored in various electronic devices and online information systems, including computers, smartphones, tablets, smartwatches, electronic appliances, portable media (e.g. USB sticks, external hard drives) and clouds, associated with individuals suspected or accused of criminal offences, as well as those in the possession of other individuals. It also concerns electronic data and evidence held by telecommunication and internet service providers registered in domestic or foreign jurisdictions. However, it does not address legal and/or practical considerations related to interception and obtaining real-time electronic data and evidence from telecommunications operators, and refrains from exploring issues concerning the collection of electronic data (and evidence) through techniques of mass surveillance, as well as strategies like 'predictive risk-assessment' or other similar approaches aimed at preventing crime and enhancing law enforcement capabilities.

First, the Toolkit briefly overviews selected projects, both completed and ongoing, along with guidance documents relevant to e-evidence. Then, it explores the international and EU legal framework and delves into the presumption of innocence and fair trial rights of individuals suspected and accused in criminal proceedings. Turning its focus to e-evidence, the Toolkit then introduces the definition, origins, types, and various phases in the life cycle of e-evidence. This general introduction concludes by delving into efforts aimed at harmonising legal practices and establishing standardised European procedures for handling e-evidence.

The main Section begins by focusing on the pre-trial investigation stage of criminal proceedings, exploring the acquisition/collection, preservation and analysis of electronic data and evidence by law enforcement agencies. It examines each phase in the e-evidence life cycle while exploring the procedural roles played by prosecutors, defence lawyers and investigating judges. It also acknowledges the delicate balance that must be found between the presumption of innocence, procedural fairness and privacy on the one hand, and the demands of digital forensics and desire for efficient criminal persecution of perpetrators of criminal acts on the other.

Attention is then shifted to e-evidence during the trial stage, where the focus is placed on the judicial assessment of the admissibility of e-evidence. Covering two distinct aspects, the non-use of certain evidence during trial, as well as the exclusionary rule, admissibility of evidence is not only a technical rule but one that is also often connected to the main constitutional principles of a national legal order, including the prohibition of torture and the right to a fair trial. The Toolkit observes a twofold approach in Europe, namely legal systems strictly filtering the information to be admitted at trial (so-called 'controlled systems') and legal systems, leaving it to the judge to assess whether it is appropriate to disregard illegal evidence ('free proof systems'). Although the Treaty on the Functioning of the European Union identifies the issue of admissibility as a domain within the EU's competence in criminal law, and certain initial steps in this regard are evident in certain legislative instruments and Court of Justice of the European Union judgments, this has not led to the creation of an EU legislative text. Given the absence of a unified EU approach, the primary common criteria regarding the admissibility of evidence are still grounded in the requirements set forth by the European Convention on Human Rights and the judgments of the European Court of Human Rights.

Finally, the Toolkit tackles the cross-border sharing of e-evidence by focusing on the European Investigation Order (EIO) and the recently adopted 'EU e-evidence system', which introduces the European Production Order and European Preservation Order for e-evidence in criminal matters. The Toolkit focuses on the main aspects of these instruments, including their application scope, types of electronic data covered, conditions for issuance, obligations of the ordering and executing states, grounds for non-recognition, legal remedies, and issues related to admissibility. After presenting each instrument, it offers a set of recommendations for practitioners. These recommendations highlight specific considerations to keep in mind when making use of these instruments. While the discussion of these instruments is essential to understand the horizontal approach of EU criminal law instruments, the main feature of the new e-evidence system under Regulation (EU) 2023/1543 and Directive (EU) 2023/1544 is the direct issuance of Preservation and Production Orders from one Member State to a telecommunication provider in another, without the participation of authorities from the second Member State. The second State involves itself only in the case of certain categories of data, provided the case is not considered 'domestic' and there are problems with enforcement.

The Toolkit incorporates checklists of key points relating to each aspect and stage covered, prompting practitioners to reflect on the diverse legal and practical issues present when dealing with e-evidence, with particular emphasis placed on ensuring the effective implementation of the presumption of innocence and fair trial rights.

1. INTRODUCTION AND BACKGROUND

1.1. ABOUT INNOCENT

The **INNOCENT project** aims to enhance the application of the presumption of innocence when handling electronic evidence. It specifically concentrates on the effective use of electronic evidence, prioritising improvements in applying the presumption of innocence, and reinforcing other procedural safeguards for individuals suspected or accused of crimes to uphold the fairness of criminal proceedings. The project's stakeholders encompass key actors within the criminal justice systems of participating countries, such as judges, including investigating judges and prosecutors, and defence lawyers, including legal aid practitioners. The INNOCENT project is funded by the European Commission under the JUST Programme and is implemented by an international consortium comprising six partner organisations.

This Toolkit is a product of the *INNOCENT project*, which aims to enhance the application of the presumption of innocence when handling electronic evidence. **Funded by the European Commission under the JUST Programme, the project commenced in May 2022. It specifically concentrates on the effective use of electronic evidence, prioritising improvements in applying the presumption of innocence and reinforcing other procedural safeguards for individuals suspected or accused of crimes to uphold the fairness of criminal proceedings.**

The INNOCENT project is implemented by an international consortium comprising six partner organisations based in Bulgaria, Croatia, Slovenia, Poland, Slovakia, and the Czech Republic.[1] Specifically focusing on Central and Eastern European countries, the project aims to systematically analyse the similarities, best practices and challenges in the region related to the practical application of the presumption of innocence when applying electronic evidence in criminal proceedings. Additionally, the project seeks to strengthen cooperation among neighbouring jurisdictions concerning the intersection of the presumption of innocence and electronic evidence.

The project's stakeholders encompass key actors within the criminal justice systems of participating countries, such as judges, including investigating judges and prosecutors, and defence lawyers, including legal aid practitioners. Aimed at increasing the capacity of these target groups' representatives, the project seeks to perform in-depth research into the crosslink and balance between the presumption of innocence and electronic evidence. It seeks to engage target groups' representatives in a co-creation process leading to the outline of capacity building and policy recommendations in view of the practical implementation of European Union (EU) and international legislation in the context of e-evidence. **The main objectives pursued by INNOCENT also include delivering a practical tool aimed at the target groups in terms of the handling e-evidence, its admissibility in court and its implications on the presumption of innocence;**

1 Adam Mickiewicz University Poznań; Poland, Bratislava Policy Institute, Slovakia; CEELI Institute Czech Republic; Human Rights House Zagreb Croatia; Science and Research Centre Koper Slovenia; and Law and Internet Foundation Bulgaria, serving as the project's lead partner.

formulating policy recommendations on the national and pan-EU level with regards to the practical implementation of the presumption of innocence enshrined in the context of e-evidence application; and promoting the project results across and beyond the partner countries and target groups.

Throughout the project's implementation, researchers from the partner organisations engaged in various activities. These included conducting secondary research, developing co-created training materials, and organising national and international capacity-building events—both in-person and online—as well as webinars tailored to judges, prosecutors, and defence lawyers. Notably, the project partners systematically identified existing knowledge on electronic evidence and the presumption of innocence. This knowledge was sourced from prior research conducted under EU-funded projects and other initiatives, in addition to literature and reports from international and EU monitoring and research institutions.

The project also involved a thorough examination of the international and EU legal frameworks, as well as a review of the legal regulations of the participating countries and relevant international, EU, and domestic case law concerning the acquisition of electronic data and evidence, and its application in criminal courts. These comprehensive analyses enabled the project partners to pinpoint specific fields and questions that warranted further exploration, subsequently informing the agenda for capacity-building events. Building upon these activities and insights gathered from stakeholders, this Toolkit has been crafted with an aim to enhance the knowledge and skills of judges, prosecutors, and defence lawyers from participating countries, empowering them to adeptly implement the presumption of innocence and its fundamental principles when handling electronic evidence.

1.2. OBJECTIVES, SCOPE, AND STRUCTURE OF THE TOOLKIT

The **primary objective of this Toolkit** is to offer comprehensive guidance and enhance the skills and knowledge of judges, prosecutors, and defence lawyers concerning the procedural rights of individuals suspected or accused of crimes. Specifically, it focuses on the fundamental right to be presumed innocent until proven guilty, particularly in criminal cases relying on electronic evidence. The aim is to elevate comprehension of distinct legal and practical issues and challenges inherent in various phases of the electronic evidence life cycle. Furthermore, the Toolkit aspires to furnish practical guidance for handling electronic evidence throughout both the pre-trial and trial stages of criminal proceedings.

The Toolkit is designed to enhance and empower the knowledge, skills, and sensitivity of actors in criminal proceedings for fostering the presumption of innocence and fair trial rights in the realm of electronic evidence throughout its entire life cycle. This encompasses the phases of acquisition, preservation and analysis of electronic evidence by Law Enforcement Agencies (LEAs), judicial assessments of admissibility, and the exchange of electronic evidence. Initially, the Toolkit provides a concise overview of the INNOCENT project, alongside other relevant projects and guidance documents related to electronic evidence. The international and EU legal frameworks and the role of the presumption of innocence in criminal proceedings pertaining to electronic evidence are presented from a broad perspective. Subsequently, each phase in the life cycle of electronic evidence is explored individually, offering relevant information to criminal justice practitioners, specifically judges, prosecutors, and lawyers, for the adept handling of electronic evidence and to elevate the presumption of innocence and ensure a fair trial for individuals suspected or accused of crimes.

The Toolkit aims to enhance understanding of the challenges encountered by legal professionals in the acquisition, preservation and forensic analysis of electronic evidence conducted by LEAs, as well as the evaluation of admissibility of electronic evidence by judges when adjudicating criminal cases. Additionally, it addresses the cross-border access to and exchange of electronic evidence. Exploring each phase in the electronic evidence life cycle, it concentrates on the suspect's and accused person's rights to be presumed innocent until proven guilty across various stages of criminal proceedings. To facilitate a deeper understanding, the Toolkit incorporates checklists of key points relating to each aspect and stage covered. These checklists prompt readers to reflect on the diverse issues entailed in ensuring the effective implementation of the presumption of innocence and fair trial rights.

The Toolkit is based on deliverables D2.1 INNOCENT Report and D2.2 INNOCENT Case Law Analysis of Work Package 2 (WP2) 'Comparative Analysis of Data' and other outputs of the INNOCENT project. Accordingly, it draws on the findings of a background study analysing EU-funded and other completed and ongoing projects, the Council of Europe (CoE) and EU legal frameworks and case law, scientific literature and policy papers such as reports of competent EU and international bodies and NGOs related to electronic evidence.[2] It also draws on the feedback gained from INNOCENT capacity-building activities (national and international workshops) where participants were asked to share their feedback with the project partners and answer the questionnaire with regard to the elaboration of this Toolkit.[3]

Similar to some previous projects, INNOCENT brought to light instances where LEAs and judges bypassed the presumption of innocence and procedural safeguards of the suspects and accused persons, particularly due to the absence of legal representation in the early stages of proceedings. In some cases, cooperation of suspects or the accused persons with LEAs is strongly encouraged or coerced through threats or promises. Recognising the substantial implications of these findings on the gathering and application of electronic evidence, the Toolkit is designed to enhance practitioners' knowledge and awareness in the realm of electronic evidence and new technologies. The emphasis is on strengthening the presumption of innocence and ensuring a fair trial, while also recognising the need of effective prosecution of crime.

2 See INNOCENT Report, INNOCENT – Improving the presumption of innocence when handling electronic evidence, WP2: Comparative Analysis of Data, D.2.1, prepared by the Adam Mickiewicz University Poznań.

3 When asked about the potential usefulness of such a document for prosecutors, defence lawyers, and judges in their respective roles, participants indicated that while creating a single tool or manual for these groups would be highly valuable, it presents significant challenges, mainly due to the inherent conflicting interests between the defence and prosecution. However, they emphasised that a manual on handling electronic evidence would be an exceptionally beneficial tool for all participants in criminal proceedings. Participants argued that having such guiding document would provide defence lawyers with a tangible mechanism to attempt to influence the exclusion of specific evidentiary material from the case file. For prosecutors, clear instructions in the pre-trial stage for lawfully collecting electronic evidence would be crucial for ensuring a quality indictment. Additionally, the courts would find it considerably easier to assess the legality and evidentiary value of the presented evidence.

Furthermore, the research showed that electronic evidence faces resistance in court, with judges often exhibiting scepticism and seeking additional assurances compared to other forms of evidence. One significant reason for the reluctance to accept electronic evidence in trials is the limited understanding among judges and prosecutors regarding the nature and technical characteristics of electronic evidence. Additionally, many professionals in the legal field lack sufficient training in the collection and handling of electronic evidence.

It is also noteworthy that **during the national capacity building events, the discussions in which participants engaged pointed to a noticeable divergence in perspectives among different criminal justice actors. Defence lawyers, as expected, brought attention to violations of the presumption of innocence and fair trial rights, expressing concerns about LEAs tendency towards impeding the effective defence of suspects and defendants. Conversely, prosecutors highlighted the challenges arising when criminals make use of a wide array of electronic devices, while LEAs lack effective legal and technical tools for investigation. Emphasising that there has been considerable academic focus on the 'hypothetical' risk of electronic evidence misuse and violation of rights of suspects and accused persons, they highlighted the need for more attention to practical problem-solving.**[4]

Like the INNOCENT project, **this Toolkit is specifically tailored for criminal justice practitioners operating in Central and Eastern Europe (i.e. in the countries actively involved in the project).** It focuses on the application of the presumption of innocence throughout the processes of collection, preservation, forensic analysis, judicial evaluation, and cross-border exchange of electronic evidence. Its primary goal is to foster improved dialog among legal practitioners within the jurisdictions of these countries on issues concerning the application of the presumption of innocence (and fair trial rights) when handling electronic evidence.

This Toolkit focuses on issues related to the presumption of innocence and the fair trial rights in the context of acquiring, preserving, analysing, evaluating, and sharing electronic information and data stored on various electronic devices. These devices encompass a broad range, including computers, smartphones, tablets, smartwatches, electronic appliances, SIM cards, memory cards, and portable media (e.g. USB sticks and external hard drives), as well as data stored in the cloud or on online information systems. The scope of this Toolkit extends to electronic data and evidence found on devices or remote locations associated with individuals suspected or accused of criminal offences, as well as those in the possession of other individuals. Furthermore, it encompasses data and evidence held by telecommunication and internet service providers registered in domestic or foreign jurisdictions.

The Toolkit concerns stored subscriber, traffic, and content data directly associated with a specific criminal offence under investigation. Notably, **it does not address legal and/or practical considerations related to obtaining real-time electronic data and evidence from telecommunications operators. Furthermore, it refrains from exploring issues concerning the collection of electronic data (and evidence) through techniques of mass surveillance, as well as strategies like 'predictive risk-assessment' or other similar approaches aimed at preventing**

4 For example, during the workshop in Slovenia, a participating prosecutor shared the perspective that while academic discussions on the necessity of protecting human rights are interesting, it is equally crucial to ensure the safety and security of citizens and deliver justice to crime victims. As a public prosecutor, he expressed concern about the 'sometimes impractical views of experts from academia on the need to elevate human rights standards, especially the right to privacy of communications.' The prosecutor lamented that these views are frequently and swiftly put into practice, not only by defence lawyers who find them advantageous but also by judges seeking innovation in their rulings to demonstrate alignment with legal scholarship advancements. In the opinion of the prosecutor, 'this trend results in an increasingly inefficient criminal procedure and an unreasonably high level of protection for individuals who, from the outset, intended to use a specific means of communication for criminal purposes.'

crime and enhancing law enforcement capabilities. These methodologies naturally prompt questions regarding the proportionality of interference with human rights as significant as those tackled by this Toolkit.

In the initial Sections of this Toolkit, the focus is first placed on providing a brief overview of selected projects, both completed and ongoing, along with guidance documents relevant to electronic evidence. It explores the international and EU legal frameworks, as well as the definition, origins, types, and various phases in the life cycle of electronic evidence. Subsequently, the Toolkit delves into efforts aimed at harmonising legal practices and establishing standardised procedures for handling electronic evidence. The introductory/general part concludes by delving into the presumption of innocence and fair trial rights of individuals suspected and accused in criminal proceedings.

The main Section explores the three segments of criminal proceedings. First, it focuses on the pre-trial stage of criminal proceedings, specifically the acquisition/collection, preservation, and analysis of electronic data and evidence. It investigates the legal framework governing these processes, examining each phase in the electronic evidence life cycle in detail while acknowledging the delicate balance required between procedural fairness on the one hand and the demands of digital forensics on the other.

It then shifts its attention to electronic evidence during the trial stage. This involves the assessment of authenticity, lawfulness, and admissibility of electronic evidence by the courts, with judges playing a pivotal role.

Finally, it tackles the cross-border access to and sharing of electronic evidence. It introduces the so-called 'EU e-evidence system', focusing on the European Investigation Order (EIO) in the context of cross-border electronic evidence collection and exchange, and the recently adopted European Production Order and European Preservation Order for electronic evidence in criminal matters. The Toolkit concludes with a summary of the contents.

2. EVIDENCE IN THE DIGITAL AGE: KEY HIGHLIGHTS FROM OTHER PROJECTS AND GUIDANCE DOCUMENTS

As digital technologies become omnipresent in contemporary societies, their impact on criminal proceedings is undeniable. Several reports highlight that **90% of criminal proceedings nowadays have a digital element and that evidence in an electronic form is increasingly present and accepted by the courts.[5] Becoming an essential element of the criminal law and criminal proceedings landscape, electronic evidence introduces a host of challenges for criminal justice actors.**

Given that such evidence can originate from a wide range of sources, such as smartphones, computers, social media, cloud services, and Internet of Things (IoT) devices, handling and interpreting evidence from these diverse sources require specialised knowledge and skills. When considering that judges, prosecutors and defence lawyers may lack the necessary technological expertise, the necessity for collaboration with digital forensics experts becomes apparent.

In their daily practice, criminal justice actors must deal with the challenge of verifying the source and chain of custody to ensure the evidence's reliability and meet specific legal standards for admissibility. Since these may vary across jurisdictions, electronic evidence and those who handle it are also faced with challenges related to mutual legal assistance and the recognition of foreign evidence in legal proceedings.

The new 'digital reality' has also led to the increasing use of encryption technologies which can hinder the ability to access and interpret digital evidence, raising concerns about balancing the presumption of innocence, fair trial rights and privacy on the one hand, and law enforcement needs on the other.

These factors, combined with a multitude of other challenges associated with electronic evidence, underscore the need for continuous training among legal practitioners, supported by professional and scientific literature, as well as capacity building evets and research projects to stay abreast of developments in this rapidly evolving field.

The INNOCENT project also discovered, *inter alia*, that among sources such as toolkits and toolboxes, handbooks, roadmaps, and other guidance documents that emerged as a result of EU-founded and other international projects targeting criminal justice practitioners, none of them directly nor exclusively related to electronic evidence with an emphasis on the strengthening presumption of innocence. Nevertheless, some projects and their deliverables do refer, from different perspectives, either to electronic evidence or to the presumption of innocence and other procedural rights of suspects and accused persons. This Section provides a summary of the key highlights f projects and documents that we deem relevant within the scope of this Toolkit.[6]

Taking *FORMOBILE*[7] as our starting point, the project sought to address a forensic investigation chain targeting mobile devices, providing practitioners with legal and technical knowledge about mobile devices alongside information on how to acquire electronic evidence from them. The *Guidance to Checklist Preparation for Legal Practitioners*,[8] a document completed as part of the FORMOBILE

5 See R. Stoykova: Digital evidence: Unaddressed threats to fairness and the presumption of innocence, Computer Law & Security Review 43 (2021), p. 2, https://www.sciencedirect.com/science/article/pii/S0267364921000480.

6 The content of this Section is related to the INNOCENT Report.

7 From mobile phones to court – A complete FORensic investigation targeting mobile devices (FORMOBILE), https://cordis.europa.eu/project/id/832800.

8 FORMOBILE Guidance to Checklist Preparation for Legal Practitioners, FORMOBILE: From mobile phones to court, April 2022.

project in Spring 2021, seeks to enable legal practitioners to draft their own checklist guidance documents outlining the essential actions that must and must not be taken during specific proceedings of a case. This ensures the admissibility, relevance, and probative value of digital evidence obtained from mobile devices. Such checklist guidance documents should enable legal practitioners to deal with processing mass digital data into criminal evidence in a way that guarantees the admissibility, reliability and probative value of the digital data in court. The *Guidance to Checklist Preparation for Legal Practitioners* provides actors in criminal proceedings with the checklist of questions at the pre-acquisition stage and all of the further stages of proceedings. It can serve as a handbook for all criminal justice practitioners to assess the data acquired from electronic devices.[9]

Mobile Forensics – The File Format Handbook,[10] a further publication stemming from the FORMOBILE project, summarises knowledge about various file formats and file systems common in mobile devices. According to the authors, this handbook isn't solely intended as a toolbox for investigators with extensive expertise in digital investigations. Instead, the handbook is also aimed at people who are new to digital forensics and are interested in the general theory of file recovery and file systems. It is organised into two distinct parts. Part I describes several different file systems that are commonly used in mobile devices, such as the APFS, Ext4, F2FS, QNX6 and QNX, while Part II describes five different file formats that are commonly used in mobile devices. The SQLite is practically omnipresent in mobile devices. Another important file format in the mobile world is Property Lists (they are particularly present on Apple devices). Java Serialization is a popular technique for storing object states in the Java programming language. App developers often resort to this technique to make their application state persistent. The Realm database format has emerged over recent years as a possible successor to the now ageing SQLite format and is increasingly used on mobile devices. Protocol Buffers provide a format for taking compiled data and serialising it by turning it into bytes represented in decimal values. This technique is also often used on mobile devices.[11]

The third FORMOBILE document which was found to be relevant to both INNOCENT and this Toolkit, is the *Criminal Procedure Report*.[12] The report is a product of a mixed approach which includes a literature review, case law analysis, an expert questionnaire, validation interviews, and an evaluation of legislation and analysis. It aims to assess the current criminal procedure legislation and human rights standards in regard to electronic evidence extracted from mobile devices. More specifically, it analyses how mobile forensic tools aimed at retrieving, decoding, analysing and presenting information from a mobile device is regulated in EU Member States and certain other countries, and how their legal regulation correlates with the applicable international and EU legislation. The report sets the ground for further action in response to the results from FORMOBILE to be compliant with the rules for admissibility of evidence.

Another relevant guidance document, the *Roadmap*,[13] represents the outcome of the *EVIDENCE project*.[14] It is intended to be a resource for legislators, policymakers, LEAs and any other stakeholders with an interest in electronic evidence and is designed to be used when rethinking current policies and legislation, drafting new legislation or when looking for practical ways of addressing issues that have been identified during the research of the EVIDENCE project. Based on the main findings of the EVIDENCE project, the document focuses its attention on providing solutions for the challenges identified by the EVIDENCE project. The EVIDENCE project highlighted that although electronic evidence

9 Ibid., pp. 4–5. See also the INNOCENT Report, supra, p. 18.

10 Ch. Hummert and D. Pawlaszczyk (eds.): Mobile Forensics – The File Format Handbook. Common File Formats and File Systems Used in Mobile Devices, Common File Formats and File Systems Used in Mobile Devices, Cham: Springer, 2022, https://link.springer.com/book/10.1007/978-3-030-98467-0.

11 Ibid., p. vii.

12 The Criminal Procedure Report, From mobile phones to court (FORMOBILE), D2.2, December 2022.

13 Roadmap (EVIDENCE), D9.2, https://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d9-2-426.pdf.

14 European Informatics Data Exchange Framework for Courts and Evidence (EVIDENCE), https://www.evidenceproject.eu.

represents increasingly key evidence in criminal proceedings, there is no comprehensive legal framework in regard to electronic evidence collection, preservation, storage, use or exchange. The lack of such legal framework leaves LEAs grappling with a disparate array of solutions, be it legal, data protection, enforcement or technical solutions. The stakeholders involved in the project feel a need for the creation of certification and specific expertise of the persons involved in and environments where electronic evidence is preserved, stored, analysed and exchanged.[15]

The EVIDENCE project emphasised that investing in proper digital forensic tools is more than necessary, particularly considering security challenges such as the volatile nature of data, difficulties to prove authenticity and possible manipulation which make proper investigative tools a necessity for all LEAs. It also highlighted that there is a lack of technical knowledge, experience and training within the judiciary as well as among prosecution and defence lawyers. For them, it also proves challenging to stay up to date with all the innovations and tools, and it is therefore desirable for every judicial actor to be trained in order to guarantee a minimum base knowledge on electronic data and its use in the judicial system. This will streamline operations, minimising time and resource wastage while simultaneously fostering trust. According to the authors of the EVIDENCE project, this needs to be addressed through mandatory training (on technical issues and digital forensics) for the judiciary in the field of electronic evidence. Coordinated European training programmes should also be set up and carried out within the MS to train judiciary officials within the field of electronic evidence. Furthermore, it is also advisable to compile more information on the subject matter and develop a (cyber)crime repository, including a repository of case law and lessons learnt.[16]

The EVIDENCE project identified key challenges associated with the acquisition, preservation, use, and exchange of electronic evidence. These challenges encompass a range of issues, such as a lack of trust among judicial authorities towards electronic evidence and concerns related to competencies and professional qualifications (including insufficient experience among operators, a shortage of training programmes, and a lack of specific skills within local law enforcement). Additional obstacles highlighted by the project include security concerns, fragmentation, the isolation of technological processes, cultural and personal resistance (including difficulties in adapting to technological advancements in the electronic evidence field and a failure to recognise its unique characteristics), and governance-related issues (such as the absence of specialised judicial services, the assignment of cases to judges lacking expertise, challenges in the relationship between law enforcement agencies and international server providers, difficulties stemming from the non-binding nature of international cooperation, and jurisdictional limitations). Furthermore, the authors of the EVIDENCE project underscore challenges of a functional nature, such as the absence of established procedures or guidelines for obtaining, preserving, and presenting electronic evidence, as well as the overwhelming quantity of data necessitating thorough analysis. In response to these identified obstacles, the project advocates for the implementation of supportive policies, the creation of a favourable technological and professional environment, and the promotion of initiatives aimed at facilitating the effective introduction and management of electronic evidence. [17]

In crafting this Toolkit, the researchers considered the findings and outcomes of both prior and ongoing EU and other initiatives. The *PRESENT project*,[18] for example, focused on enhancing the right to be present at trial for individuals

15 Ibid. See also the INNOCENT Report, supra, pp. 13–17.

16 Ibid.

17 Ibid.

18 Enhancing the Right to be Present (PRESENT), https://www.netlaw.bg/en/a/enhancing-the-right-to-be-present-present.

facing criminal allegations and enhancing certain aspects of the presumption of innocence. Among its achievements is a comparative analysis assessing the extent to which Directive 2016/343 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial[19] has been implemented in the six participating countries. This analysis not only highlights the successful implementation of minimum procedural safeguards, but also exposes shortcomings and gaps in adherence to the Directive.[20]

The main output of the PRESENT project, the *Recommendation List*, [21] outlines measures deemed most successful and effective in implementing and applying the Directive, applicable across all participating countries. This deliverable targets decision-makers and policy influencers, offering expert opinions and practical solutions for amending legislation to achieve uniformity and heightened efficacy of legal remedies. Furthermore, the PRESENT project led to the development of a national concept for electronic justice, aiming to ensure equal protection of procedural rights in both electronic and traditional paper-based formats.[22]

Another comparative analysis to assess the practical implementation of Directive 2016/343 was carried out under the *FAIR project*,[23] which had the primary objective of improving the fairness of trials for individuals suspected or accused of crimes. Findings from the project's studies in the participating countries[25] can be found in *Enhancing the Fair Trial for People Suspected or Accused of Crimes. Best Practices Handbook*.[24] The Report reveals instances where LEAs and judges, exploiting the absence of legal representation in the early stages of proceedings, bypassed the presumption of innocence rule. This was often achieved through encouragement or coercion, involving threats or promises to induce cooperation of the defendant. This was often achieved through strong encouragement or coercion, involving threats or promises to induce cooperation of the defendant. While the case law studies conducted by the FAIR project did not specifically focus on the acquisition of electronic evidence, the observed tendency of misconduct serves as a cautionary signal. It suggests that similar situations may arise concerning the obtaining of passwords, searching electronic devices, preserving electronic data, handling electronic evidence, etc.[26]

The role of the defence lawyer from the early stage was strongly emphasised as the guarantee of the presumption of innocence. However, the analyses showed that there were various approaches followed by the countries when it came to the suspect's or accused's right to remain silent and right to not incriminate themselves in criminal proceedings. A common finding regarding Bulgaria and Hungary highlighted the pressure that may be exercised on persons suspected or accused of crimes, encouraging them to confess or agree to testify in exchange for assistance from authorities. Another finding (regarding Austria and Greece) that could be considered as widespread was that the right to remain silent was poorly communicated in practice (hence, in Greece the suspected or accused persons do not make use of this right out of fear that it will have a negative impact on their case).[27]

The *Best Practice Handbook*,[28] another deliverable linked to the FAIR project, is aimed at providing selected criminal justice practitioners, particularly police officers, prosecutors, judges and lawyers, with recommendations for their daily work to improve the fairness of trials for individuals suspected or accused of crimes. Moreover, the handbook includes precise and up-to-date information regarding the implementation of six EU Directives (Procedural Roadmap) in

19 Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, OJ L 65, 11.3.2016, p. 1–11.

20 See the INNOCENT Report, supra, pp. 20–21.

21 Recommendation list, Enhancing the Right to be Present (PRESENT), D3.4, https://www.netlaw.bg/p/r/e/recommendation-list-2467.pdf.

22 See the INNOCENT Report, supra, pp. 20–21.

23 Enhancing the Fair Trial for People Suspected or Accused of Crimes (FAIR), https://www.netlaw.bg/en/a/enhancing-the-fair-trial-for-people-suspected-or-accused-of-crimes-fair.

24 Enhancing the Fair Trial for People Suspected or Accused of Crimes. Best practices Handbook. Fair Project, https://www.netlaw.bg/p/f/a/fair-best-practices-handbook-en-2374.pdf.

25 Austria, Bulgaria, Hungary and Greece.

26 See the INNOCENT Report, supra, pp. 20–21.

27 Ibid.

28 Best Practice Handbook, Enhancing the Fair Trial for People Suspected or Accused of Crimes (FAIR), D2.4, https://www.netlaw.bg/p/f/a/fair-best-practices-handbook-en-2374.pdf.

Austria, Bulgaria, Greece and Hungary, as well as about the practical challenges for the authorities and people suspected or accused of crimes alike.

The SIRIUS project[29] is an EU-funded project co-implemented by Europol and Eurojust, in close partnership with the European Judicial Network. It initially started as a cooperation initiative between the US and the EU in the field of cross-border access to electronic evidence. Since 2018, it has been funded by the European Commission. The project helps law enforcement and judicial authorities to access cross-border electronic evidence in the context of criminal investigations and proceedings. It serves as a go-to point for obtaining electronic data from service providers based in other jurisdictions. It provides a restricted platform for sharing knowledge and best practices for both the law enforcement and judiciary. It maintains an up-to-date repository of contact details of companies, focused on smaller, hard to find or sometimes inaccessible, service providers. SIRIUS products and services can be accessed via the Europol Platform for Experts (EPE). Its resources are available to law enforcement and judicial authorities from all EU Member States, as well as to non-EU countries with an operational agreement with Europol or with Eurojust. The SIRIUS community on the EPE represents all 27 Member States, promoting cooperation and support within the European Union.[30]

The project launched an interactive video game, created in partnership with CENTRIC, that involved taking the player through a terrorism investigation to learn more about lawful data requests. SIRIUS Game v.2 is one of the most true-to-life simulations for lawful data requests. SIRIUS is dedicated to shedding light on the access and use of electronic evidence in criminal investigations in the EU. It provides high-quality training through the CEPOL platform and in-person sessions, along with innovative tools to aid in online investigations. It produces an annual Digital Evidence Situation Report.

The *PROCAM project*[31] delved into the role of audio-visual recording during the questioning of vulnerable individuals to safeguard their rights, as stipulated in Directive 2013/48 on the right of access to a lawyer in criminal proceedings.[32] Among its primary objectives, the project sought to explore the connection between audio-visual recording and enhanced protection of procedural rights for vulnerable suspects and accused individuals under EU Law. This involved an in-depth analysis of the legislation and practices of 28 EU Member States concerning the audio-visual recording of interrogations, with a specific emphasis on the interrogation of children as a particularly vulnerable demographic group.[33]

In the pursuit of understanding why certain States hesitate to adopt audio-visual recording, the researchers aimed to offer constructive, evidence-based responses. By drawing on the experiences of States where recording of interrogations is widespread, the project aimed to provide insights to state officials. The country report revealed that in the EU the implementation of the Roadmap Directives (see below) has encountered challenges, with some Member States exhibiting concerning practices, such as coercing individuals suspected or accused of crimes to provide testimony—often falsely—particularly during initial interrogations and in the absence of defence lawyers. The project's findings carry significant implications for the handling and use of electronic evidence. The mandated audio-visual recording could serve as a deterrent against misconduct and violations of the presumption of innocence and the fair trial rights, including instances where individuals are compelled to disclose passwords or provide fingerprints to access electronic devices.[34]

29 SIRIUS Cross-border Access to electronic evidence, EU-ROPOL, https://www.europol.europa.eu/operations-services-innovation/sirius-project.

30 Ibid.

31 ProCam – Procedural Rights Observed by the Camera: Audiovisual Recordings of Interrogation in the EU, https://www.oijj.org/en/our-work/research/projects/procam-procedural-rights-observed-camera-audiovisual-recordings.

32 Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, OJ L 294, 6.11.2013, p. 1–12.

33 See the INNOCENT Report, supra, p. 23.

The *EVIDENCE2e-CODEX project*[35] has undertaken a comprehensive exploration of the cross-border acquisition and exchange of electronic evidence through European Investigation Orders (EIO) and mutual legal assistance (MLA) procedures across Europe, a subject highly pertinent to both the INNOCENT project and this Toolkit. In both the *Report on EIO and MLA*[36] and the *Report on the implementation of EIO*,[37] project partners highlighted the vital importance of effectively and coherently applying EIO and MLA procedures to ensure a secure and trusted exchange of information and electronic evidence in criminal cases. The project's objective was to establish a legally valid instrument for the exchange of electronic evidence related to MLA and EIO procedures over e-CODEX. It sought to equip legal and technical communities with readily usable information on EIO, electronic evidence, and e-CODEX, offering a practical example of how electronic evidence can be securely shared over e-CODEX to support MLA and EIO cases.[38]

In addressing cross-border gathering and exchange of electronic data and evidence, the project also delved into human rights issues. A key deliverable, the *Report on data protection and other fundamental rights issues*,[39] scrutinises how data protection challenges are navigated in EIO and MLA procedures. The report identifies legal and operational measures essential for upholding data protection rights, particularly concerning electronic evidence. Additionally, it examines the incorporation and handling other procedural rights, as outlined in Directive 2014/41/EU regarding the European Investigation Order in criminal matters,[40] across various EU Member States.

The *ADMISSIBILITY OF E-EVIDENCE IN CRIMINAL PROCEEDINGS IN THE EU project*[41] explored another topic which is highly important for this Toolkit. The project was carried out by the European Law Institute (ELI) between September 2022 and November 2022. The authors pointed out that at present, each EU Member State follows its own rules on criminal investigative measures for evidence gathering, resulting in different standards for its admissibility. When such evidence, including electronic evidence, is to be shared with other EU Member States, a clear mechanism governing its admissibility is needed. The project resulted in the formulation of a legislative proposal concerning the admissibility and exclusionary rules governing electronic evidence in criminal proceedings.[42] This proposal is complemented by a comprehensive background study that analyses (a) general principles surrounding the admissibility/exclusion of criminal evidence, considering diverse national approaches within selected EU Member States; (b) pertinent case law from the ECtHR; (c) the protection of lawyer-client privilege in digital searches and the cross-border implications of such searches; and (d) the identification of immunities.[43]

The INNOCENT researchers also focused on projects aimed at developing and applying technology-driven innovative measures to acquire data and information that are used as electronic evidence in the courts. These projects are aimed, *inter alia*, at combining new speech technologies, face recognition and network analysis to facilitate the identification of criminals. They also involve developing a platform to enhance agencies' capabilities in face and voice recognition through video and audio technologies[44] and are aimed at inventing new methods of evidence gathering through developing and validating a novel, ultra-sensitive and ultra-low-power, miniaturised, low-cost, wireless, autonomous and intelligent technological devices (sensors and cameras). Such high-tech devices are designed to operate at remote locations, automatically identify pre-defined criminal events, and alert LEAs in real time while providing and storing the relevant video, location and timing evidence.[45] Furthermore,

34 Ibid.

35 EVIDENCE2e-CODEX – Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe, https://evidence2e-codex.eu

36 Report on EIO and MLA (EVIDENCE2e-CODEX), D2.2, https://evidence2e-codex.eu/p/e/v/evidence2e-codex-deliverable-d2-2-summary-731.pdf.

37 Report on implementation of EIO (EVIDENCE2e-CODEX), D2.1, https://evidence2e-codex.eu/p/e/v/evidence2e-codex-deliverable-d2-1-summary-523.pdf.

38 See the INNOCENT Report, supra, p. 23.

39 Report on data protection and other fundamental rights issues (EVI- DENCE2e-CODEX), D2.3., https://evidence2e-codex.eu/p/e/v/evidence2e-codex-deliverable-d2-3-summary-436.pdf.

40 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, p. 1–36.

41 Admissibility of E-Evidence in Criminal Proceedings in the EU, https://www.europeanlawinstitute.eu/projects-publications/completed-projects/admissibility-of-e-evidence/.

42 ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings: Draft Legislative Proposal of the European Law Institute, University of Vienna, European law Institute, 2023, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf.

43 See the INNOCENT Report, supra, p. 27.

44 See ROXANNE – Real time network, text, and speaker analytics for combating organised crime, https://roxanne-euproject.org

45 See FOREnsic evidence gathering autonomous seNSOR, https://cordis.europa.eu/project/id/653355.

these projects' objective is to develop novel methods and technical solutions for investigating and mitigating illegal activities involving virtual currencies and/or underground market transactions, as well as providing low-cost and open-source tools for cryptocurrency forensics.[46]

The *TITANIUM project*,[47] for example, is notable in its aim to equip LEAs with the essential tools to identify cybercriminals, even when operating under the cloak of pseudo-anonymity provided by virtual currencies. Through the development of low-cost and open-source tools, TITANIUM enhances investigative capabilities for LEAs in virtual currency and darknet market analytics, surpassing the simplicity of current methods employed by many investigators. This advancement promises improved overall capabilities, expedited investigations, and cost-effectiveness for Europe as a whole. The outcomes of projects like TITANIUM, centred around emerging technologies, have been acknowledged by the authors as highly relevant to the INNOCENT project and this Toolkit. Their substantial potential lies in the development of tools for acquiring electronic evidence to be used in criminal proceedings. However, while enhancing the efficiency of LEAs in obtaining e-evidence is crucial, this imperative must not be enforced at the cost of safeguards to protect fundamental rights, such as the right to fair trial and privacy.[48]

In synthesising insights gleaned from other projects, consulting various guidance documents, scrutinising extensive scientific literature, and comprehensively reviewing legal frameworks and case law at national, international, and EU levels, the INNOCENT project aimed to facilitate capacity-building events. This included organising training sessions, workshops, and webinars tailored for judges, prosecutors, and defence lawyers across the six participating countries.

Furthermore, drawing upon knowledge and feedback accumulated through national and international events, as well as insights gathered from participants about their specific needs and expectations, the members of the research consortium have crafted this Toolkit. Representing one of the pivotal deliverables of the INNOCENT project, this Toolkit serves as a culmination of insights, experiences, and collaborative efforts to address the multifaceted challenges within the realm of electronic evidence and its application in criminal proceedings.

46 See the INNOCENT Report, supra, p. 25.

47 Tools for the Investigation of Transactions in Underground Markets, https://cordis.europa.eu/project/id/740558.

48 See the INNOCENT Report, supra, p. 26.

3. THE INTERNATIONAL AND EU LEGAL FRAMEWORK - AN OVERVIEW

3.1. THE COUNCIL OF EUROPE LAW

Several crucial legal instruments within the Council of Europe merit careful consideration in relation to electronic evidence and its intersection with the presumption of innocence and other fundamental rights in criminal proceedings. Notably, these include the **European Convention on Human Rights**,[49] the **Convention on Cybercrime**,[50] and the **Second Additional Protocol to the Convention on Cybercrime**,[51] specifically addressing enhanced cooperation and disclosure of electronic evidence. Before the entry into force of the Convention on Cybercrime and the Second Additional Protocol, mutual assistance in criminal matters in the CoE was governed by the European **Convention on Mutual Assistance in Criminal Matters**[52] (CoE MLA Convention). This Convention was supplemented by the **Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters**.[53]

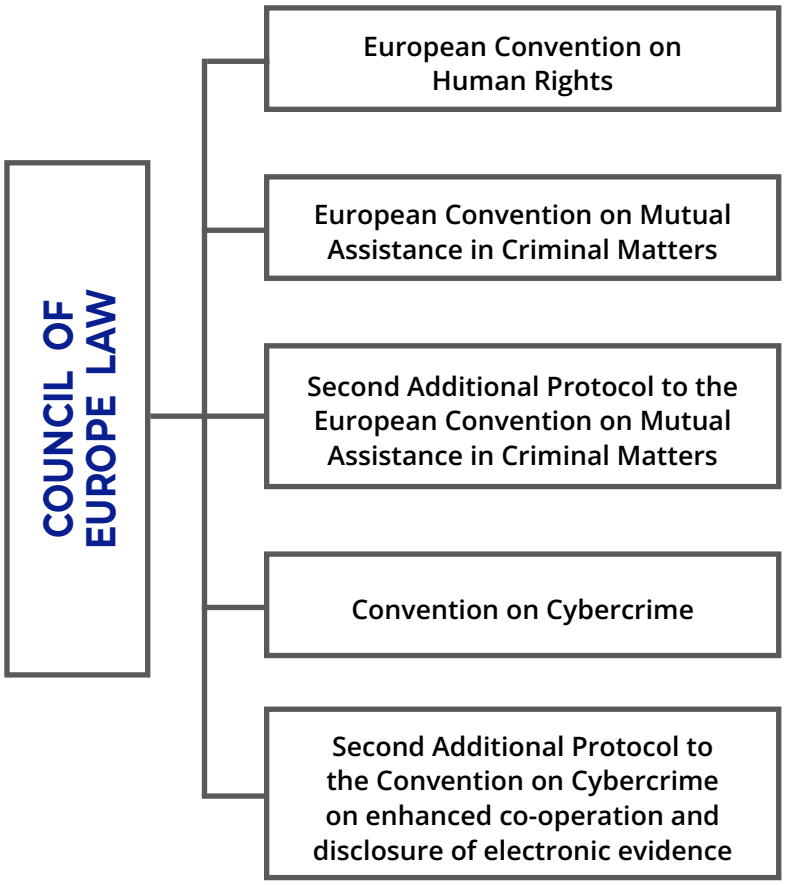

Figure 1: Council of Europe law related to electronic evidence

49 European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos 11 and 14, Council of Europe, ETS 5, 4 November 1950, https://www.echr.coe.int/documents/d/echr/convention_ENG.

50 Convention on Cybercrime, Council of Europe, ETS 185, 23 November 2001, https://www.refworld.org/docid/47fdfb202.html.

51 Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Council of Europe, CETS 224, 17 November 2021, https://rm.coe.int/1680a49dab.

52 European Convention on Mutual Assistance in Criminal Matters, Council of Europe, ETS No 030, 20 April 1959, https://rm.coe.int/16800656ce.

53 Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, Council of Europe, ETS No 182, 8 November 2001.

3.1.1. The European Convention on Human Rights

The *European Convention on Human Rights* (ECHR) is the core international legal instrument to protect human rights and political freedoms in Europe. Drafted in 1950 by the then newly formed Council of Europe, the convention entered into force on 3 September 1953. All CoE Member States are party to the convention. As amended by Protocol 11,[54] the Convention consists of three parts. The main rights and freedoms are contained in Section I, which consists of Articles 2 to 18. Section II (Articles 19 to 51) sets up the European Court of Human Rights and its rules of operation. Section III contains various concluding provisions.

The ECHR's most relevant fundamental rights that should be considered in the context of handling electronic evidence in criminal proceedings are the *right of a fair trial* (Article 6), and the *right to respect for private and family life* (Article 8). Two fundamental rights that are also relevant are the *presumption of innocence* and the *right to an adequate defence*. They are laid down in Article 6 as fair trial rights.

In line with Article 6(2) of the ECHR, anyone charged with a criminal offence shall be presumed innocent until proved guilty according to law. According to the case law of the European Court of Human Rights (ECtHR), the right of a fair trial is inextricably related to the respect of the *right to remain silent* and the *right to not incriminate oneself*, i.e. two rights which are not explicitly stipulated in the text of the ECHR. Article 6(3)(b) provides that everyone should be guaranteed to have adequate time and facilities for the preparation of their defence.

Pursuant to Article 8 of the ECHR, the private and family life, and the confidentiality of the correspondence of the individuals should be respected. This includes protecting the privacy of messages, phone calls, and e-mails. Privacy rights protect the individual and the public from unlawful and unnecessary government surveillance. Governments can only interfere with these rights when it is specifically allowed by law and done for a good reason – such as national security or public safety, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.

While each of the aforementioned rights holds significance in the processes of gathering, preserving, conducting forensic analyses, assessing legality and admissibility, as well as facilitating the cross-border exchange of electronic evidence, this Toolkit places particular emphasis on the principle of presumption of innocence.

54 There are 16 additional protocols to the ECHR altogether.

3.1.2. The Convention on Cybercrime

The Convention on Cybercrime requires States to ensure that the specific criminal offences against and by means of computers are criminalised in their domestic law and aims at harmonising the domestic criminal substantive law elements in cybercrime. It sets out the procedural powers (such as expedited preservation of stored data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of computer data; real-time collection of traffic data; and interception of content data, and determines the common conditions and safeguards, applicable to all procedural powers) necessary for the investigation and prosecution of criminal offences specified by the Convention and any other offences committed by means of a computer system and those with evidence in electronic form. The Convention also establishes a regime of international co-operation and mutual assistance.

Adopted by the Committee of Ministers of the Council of Europe on 8 November 2001, the *Convention on Cybercrime*, commonly known as the Budapest Convention on Cybercrime or the Budapest Convention, officially came into force on 1 July 2004. Recognised as the foremost international agreement addressing cybercrime and electronic evidence, it stands as a pivotal international legal instrument with global membership and impact across all regions of the world. This historic treaty delineates the criminalisation of cybercrime, procedural legal tools for investigating such crimes, and mechanisms to secure electronic evidence. Additionally, its significance lies in establishing a legal foundation for international cooperation.

The Budapest Convention on Cybercrime is designed to achieve three primary objectives:

1. harmonising the domestic criminal substantive law elements of offences and connected provisions in cybercrime;
2. providing for domestic criminal procedural law powers necessary for the investigation and prosecution of offences specified by the Convention as well as other offences committed by means of a computer system and those with evidence in electronic form; and
3. setting up a fast and effective regime of international co-operation.[55]

The Convention contains four chapters.[56] Chapter I (Article 1) addresses 'Use of terms' by introducing definitions of the four terms/concepts: 'computer system', 'computer data', 'service provider' and 'traffic data'.

Section 1 of Chapter II on 'Substantive law issues' covers both criminalisation provisions and other connected provisions in computer- or computer-related crime. It first defines nine offences grouped into four different categories and then deals with ancillary liability and sanctions. The Convention requires States to ensure that the specific criminal offences (enshrined in Articles 2-11) against and by means of computers are criminalised in their domestic law. These criminal offences include illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights.[57]

55 Convention on Cybercrime, Special edition dedicated to the drafters of the Convention (1997-2001), 4. Explanatory report to the Convention on Cybercrime, Council of Europe, March 2022, pp. 60–61, https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e.

56 Ibid., p. 61

57 Ibid.

Section 2 of Chapter II concerns 'Procedural law issues' (Articles 14-21). It first determines the common conditions and safeguards applicable to all procedural powers in this Chapter. It then sets out the following procedural powers:

- expedited preservation of stored data;
- expedited preservation and partial disclosure of traffic data;
- production order;
- search and seizure of computer data;
- real-time collection of traffic data; and
- interception of content data.

The provisions of this Section require the States to ensure that their criminal justice authorities have the powers prescribed in their procedural law not only to investigate criminal offences established in accordance with the substantive law provisions of the Convention, but also to investigate other offences committed by means of a computer system as well as any offence where evidence is in electronic form (Article 14). Any investigation making use of such legislative provisions may be attributed to the Cybercrime Convention. However, prosecutions and court decisions should refer to the articles of domestic law and not to the Budapest Convention except for instances where evidence has been obtained through international cooperation provisions. Chapter II concludes with the jurisdiction provisions.[58]

Chapter III on 'International co-operation' contains the provisions concerning traditional and computer crime-related mutual assistance as well as extradition rules. It covers traditional mutual assistance in two situations: where no legal basis (treaty, reciprocal legislation, etc.) exists between parties – in which case its provisions apply – and where such a basis exists – in which case the existing arrangements also apply to assistance under this Convention. Computer- or computer-related crime specific assistance applies to both situations and covers, subject to extra-conditions, the same range of procedural powers as defined in Chapter II. In addition, Chapter III contains a provision on a specific type of trans-border access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the States.[59]

Finally, Chapter IV contains the final clauses, which – with certain exceptions – repeat the standard provisions in Council of Europe treaties.[60]

The Convention obliges the States to make sure that the establishment, implementation and application of the powers and procedures provided for in the Convention are subject to conditions and safeguards provided for under its domestic law. These shall provide for the **adequate protection of human rights and liberties**, including rights enshrined in the ECHR, the United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments. In their domestic law, countries shall incorporate **the principle of proportionality**. Such conditions and safeguards shall, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure (Article 15).

For the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, and for the collection of evidence in electronic form, the **Convention obliges the States to co-operate with**

58 Ibid.
59 Ibid.
60 Ibid.

each other and to afford one another mutual assistance to the widest extent through the application of all relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws (Article 23).

Pursuant to Article 35 of the Convention, States should designate a point of contact available on a 24 hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of electronic evidence. The assistance through these points of contact, which form the so-**called 24/7 network of contact points**, includes facilitating, and, if permitted by its domestic law and practice, directly carrying out (a) the provision of technical advice; (b) the preservation of data; (c) the collection of evidence; (d) the provision of legal information; and (e) locating of suspects.

States that are Parties, Signatories or Invitees participate as members or observers in the *Cybercrime Convention Committee* (T-CY). The T-CY assesses, *inter alia*, implementation of the Convention, adopts recommendations to the Parties or prepares additional legal instruments. According to the T-CY and the statistics supplied by States themselves, **countries use the 24/7 network of contact points extensively. The Czech Republic, a country participating in the INNOCENT project, for example, reported on a case which was successfully resolved with the assistance of the 24/7 network. A Czech psychologist received several e-mails containing suicidal thoughts from a person using the seznam.cz portal. IP logs of the e-mail box were obtained. As soon as the provider of the e-mail service (Deutsche Telekom) was identified, immediate co-operation was requested via the German contact point, which established the endpoint of the user of the IP address. The user who had sent the e-mails was a Czech citizen living in Germany.[61] The Slovak Republic, another partner to the INNOCENT project, had 321 outgoing 24/7 messages to 13 countries in 2019, of which most to the USA (193) followed by Germany (34), the Czech Republic (29) and the UK (14). It received 380 messages, of which most from the USA (264), followed by the Czech Republic (39), Germany (22) and the UK (15).**

In 2012, the T-CY issued *Guidance Notes* aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[62] In total, there are 13 Guidance Notes that represent the common understanding of the States regarding the use of the Convention. For example, in the light of developing forms of technology that go beyond traditional mainframe or desktop computer systems, the T-CV determined the scope of the definition of 'computer system' in Article 1(A) of the Budapest Convention.[63]

According to the T-CY, the Parties, Signatories and countries which had been invited to accede to the Budapest Convention have either already reformed their domestic legislation or are in the process of doing so.[64]

61 Budapest Convention on Cybercrime: Benefits and Impact in Practice, Council of Europe, Strasbourg 13 July 2020, pp. 19–21, https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac.

62 See T-CY Guidance Notes, Adopted by the 8th, 9th, 12th, 16th and 21st Plenary of the T-CY, Council of Eu- rope, Strasbourg, 8 July 2019, pp. 4-5, https://rm.coe.int/t-cy-guidance-notes-compilation/16809fc22c.

63 Article 1(A) defines 'computer system' as any 'device or group of interconnected correlated devices, one or more of which, pursuant to a program, performs automatic processing of data'. The T-CV acknowledged that since the time of the drafting of the Convention new devices were developed such as modern generation mobile phones ('smart' phones), personal digital assistants ('PDAs'), tablets, and others that produce, process or transmit data and agreed that these devices were covered by the definition of 'computer system'. See ibid.

64 Ibid., pp. 5–7. For example, Croatia, a participating country to the INNOCENT project, brought its substantive and procedural law in line with the Budapest Convention in 2013, when new Criminal and Criminal Procedure Codes entered into force. The Slovak Republic, also a project partner to the INNOCENT, adopted two acts in 2005 that amended the Criminal Code and the Criminal Procedure Code to meet the requirements of the Budapest Convention.

CHECKLIST OF KEY POINTS ON THE CONVENTION ON CYBERCRIME

- ☐ A pivotal international legal instrument with global membership and impact across all regions of the world.
- ☐ Recognised as the foremost international agreement addressing cybercrime and electronic evidence.
- ☐ Delineates the criminalisation of cybercrime, procedural legal tools for investigating such crimes, and mechanisms to secure electronic evidence.
- ☐ Establishes a legal foundation for international cooperation.
- ☐ States should criminalise specific criminal offences against and by means
- ☐ of computers.
- ☐ States should ensure that their criminal justice authorities have the following powers: expedited preservation of stored data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of computer data; real-time collection of traffic data; and interception of content data.
- ☐ For the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, and for the collection of evidence in electronic form, the States should co-operate with each other and to afford one another mutual assistance to the widest extent through the application of all relevant international instruments.
- ☐ States should designate a point of contact available on a 24 hour, seven-day-a-week basis to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of electronic evidence.
- ☐ Sets up a '24/7 network' for ensuring speedy assistance among the States.
- ☐ There are altogether 13 Guidance Notes that represent the common understanding of the States regarding the use of the Convention.

3.1.3. The Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence

The **Second Additional Protocol**, mirroring the Convention, seeks to bolster the capacity of LEAs in combatting cyber and other forms of crime, while upholding human rights and fundamental freedom and acknowledging the significance of an internet infrastructure founded on the unimpeded flow of information. The primary aim of the Protocol is to augment collaboration in addressing cybercrime and enhancing the ability of criminal justice entities to collect electronic evidence. Its overarching objective is to introduce novel mechanisms for obtaining the disclosure of electronic evidence from another State in a 'rapidly expedited manner'. This may involve direct collaboration with service providers in that jurisdiction and the prompt release of data during emergency situations that pose threats to human lives. Simultaneously, the Protocol establishes a framework encompassing human rights and the rule of law to safeguard these tools.

Over the last two decades, the Convention on Cybercrime has been supplemented, first with the 2003 Additional Protocol addressing the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Subsequently, in 2021, the Convention was further augmented by the *Second Additional Protocol on enhanced co-operation and the disclosure of electronic evidence*.

Adopted by the Committee of Ministers of the CoE on 17 November 2021, the Second Additional Protocol was opened for signature on 12 May 2022. It seeks to provide for additional tools regarding international cooperation in criminal matters, including for cooperation in emergency situation. More particularly, **the primary aim of the Protocol is to provide for new tools to obtain the disclosure of electronic evidence in another State in a 'rapidly expedited manner' – such as through direct cooperation with service providers in that jurisdiction, as well as expedited disclosure of data in emergency situations where lives are at risk. Simultaneously, the Protocol provides for a system of human rights and rule of law safeguards for such tools, including for the protection of personal data transferred under the Protocol**.[65]

The Second Additional Protocol is the result of a complex process of negotiations spanning over almost 4 years (September 2017 to May 2021)[66] during which time the States recognised the growing use of information and communication technology, including internet services, and increasing cybercrime, a threat to democracy, human rights, and the rule of law. They recognised the growing number of victims of cybercrime and the importance of obtaining justice for those victims and recalled that governments have the responsibility to protect society and individuals against crime not only offline but also online, including through effective criminal investigations and prosecutions.[67]

Moreover, **the States expressed their awareness that evidence of any criminal offence is increasingly stored in electronic form on computer systems in foreign, multiple or unknown jurisdictions. Convinced that additional measures are needed to lawfully obtain such evidence in order to enable**

65 Second Additional Protocol to the Convention on enhanced co-operation and disclosure of electronic evidence, Special edition dedicated to the drafters of the Protocol, Council of Europe, 17 November 2021, p. 5, https://rm.coe.int/special-edition-second-protocol-en-2021/1680a69930.

66 Ibid. The contributions of over 600 experts from 75 countries and international organisations, and almost 100 negotiation sessions as well as stakeholder consultations were necessary to come to the final draft of the Protocol.

67 Second Additional Protocol to the Convention on enhanced co-operation and disclosure of electronic evidence, Special edition dedicated to the drafters of the Protocol, supra, Preamble.

an effective criminal justice response and to uphold the rule of law, they recognised the need for increased and more efficient cooperation between States and the private sector, and that in this context greater clarity and legal certainty is needed for service providers and other entities regarding the circumstances in which they may respond to direct requests from criminal justice authorities in another State for the disclosure of electronic data.[68]

The Second Additional Protocol is divided into four chapters.[69] The 'Common Provisions' of Chapter I cover the purpose and scope of the Protocol. As is the case for the Convention, the Protocol relates to specific criminal investigations or proceedings, not only with respect to cybercrime, but also to any criminal offence involving electronic evidence. This Chapter also makes definitions of the Convention applicable to the Protocol and contains additional definitions of terms that are frequently used.

Chapter II on 'Measures for enhanced co-operation' contains the primary substantive articles of the Protocol, which describe various methods of cooperation available to the States. As different principles apply to each type of cooperation, the Chapter is divided into five Sections: (1) General principles, (2) Procedures enhancing direct cooperation with providers and entities in other Member States, (3) Procedures enhancing international cooperation between authorities for the disclosure of stored computer data, (4) Procedures pertaining to emergency mutual assistance and (5) Procedures pertaining to international cooperation in the absence of applicable international agreements.[70]

Chapter III provides for 'Conditions and safeguards'. States shall also apply conditions and safeguards, such as Article 15 of the Convention, to the powers and procedures of the Protocol. In addition, this Chapter includes a detailed set of safeguards for the protection of personal data.[71]

The 'Final provisions' of Chapter IV are similar to the standard final provisions of most Council of Europe treaties. They make provisions of the Convention applicable to this Protocol. However, Article 15 on 'Effects of this Protocol', Article 17 on the 'Federal clause' and Article 23 on the 'Consultations of the Parties and assessment of implementation' differ in varying degrees from analogous provisions of the Convention. This last article, for example, provides that the effective use and implementation of the provisions of the Protocol shall be periodically assessed by the States.

The general scope of application of the Protocol is the same as that of the Convention: the measures of the Protocol are to be applied to specific criminal investigations or proceedings concerning criminal offences related to computer systems and data, as well as to the collection of evidence in electronic form. As explained in paragraphs 141 and 243 of the explanatory report to the Convention, this means that where the crime is committed by use of a computer system, or where a crime not committed by use of a computer system (a murder, for example) involves electronic evidence, the powers, procedures and cooperation measures created by the Protocol are intended to be available.[72] The Second Additional Protocol also applies to specific criminal investigations or proceedings concerning the criminal offences established pursuant to the First Protocol (i.e. offences of a racist and xenophobic nature committed through computer systems).

68 Ibid.

69 Ibid., pp. 38–39.

70 Ibid., p. 39.

71 Ibid.

72 See ibid. See also Convention on Cybercrime, Special edition dedicated to the drafters of the Convention (1997-2001), 4. Explanatory Report to the Convention on Cybercrime, supra, p. 83.

In terms of substance, a particular concern in relation to the Protocol are the challenges of territoriality and jurisdiction related to electronic evidence, given that specified data needed in a criminal investigation may be stored in multiple, shifting or unknown jurisdictions ('in the cloud'). Solutions are therefore needed to obtain the disclosure of such data in an effective and efficient manner. While Article 18 of the Convention already addresses some aspects of obtaining subscriber information from service providers (obtaining subscriber information through mutual assistance in most cases is not effective and overburdens the mutual assistance system), including in other States, the Protocol provides for **complementary tools to obtain domain name registration information and the disclosure of subscriber data directly from a service provider in another State**. As an information needed to identify the user of a specific e-mail, social media account or of a specific Internet Protocol (IP) address used in the commission of an offence, *subscriber data* is the most often sought-out information in domestic and international criminal investigations relating to cybercrime and other crimes involving electronic evidence. Without this information, which is normally held by service providers, it is often impossible to proceed with an investigation.[73]

At the time of drafting the Protocol, mutual assistance requests were the primary method to obtain electronic evidence of a criminal offence from other States, including the mutual assistance tools of the Convention. However, mutual assistance is not always an efficient way to process an increasing number of requests for volatile electronic evidence. Therefore, the Protocol introduces a more streamlined **mechanism for issuing orders or requests to service providers in other States to produce subscriber information**.[74]

As many forms of crime online are facilitated by domains created or exploited for criminal purposes, it is necessary to identify the person who has registered such a domain. Such information is held by entities providing domain name registration services. Therefore, the Protocol provides for an efficient **framework to obtain the information from relevant domain name registrars and registries in other States**.[75]

The protocol also makes reference to emergency situations, i.e. where there is a significant and imminent risk to the life or safety of any natural person, by calling upon States to provide for **emergency mutual assistance** and making use of the **points of contact for the 24/7 Network** established under the Convention (see *supra*).[76]

Outside the scope of the Protocol, important measures, such as video conferencing or joint investigation teams, are already available under treaties of the Council of Europe (for example, the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters) or other bilateral and multilateral agreements. However, such mechanisms are not universally available among Parties to the Convention, and the Protocol therefore aims to fill that gap. The tools which are introduced by the Protocol increase the efficiency of the process and relieve pressure on the mutual assistance system.

- In addition to provisions on powers and procedures related to criminal investigations and prosecutions, the Protocol contains **provisions on conditions and safeguards that ensure adequate protection of human rights and fundamental freedoms**, like those in the Convention. Recognising the requirement in many States to protect privacy and

73 Second Additional Protocol to the Convention on enhanced co-operation and disclosure of electronic evidence, Special edition dedicated to the drafters of the Protocol, supra, pp. 36–38.

74 Ibid.

75 Ibid.

76 Ibid.

personal data to meet their constitutional and international obligations, the protocol provides for **specific data protection safeguards**.

These data protection safeguards complement the obligations of many of the Parties to the Convention, which are also Parties to the Convention for the Protection of Individuals regarding Automatic Processing of Personal Data.[77]

After thorough discussion among the drafters, measures such as 'undercover investigations by means of a computer system' and 'extension of searches' were not retained in the Protocol. The drafters (i.e. the State Parties) found these measures to require additional work, time and consultations with stakeholders to be pursued in a different format and possibly in a separate legal instrument.[78]

CHECKLIST OF KEY POINTS ON THE SECOND ADDITIONAL PROTOCOL TO THE CONVENTION ON CYBERCRIME

- ☐ Provides for tools to obtain the disclosure of electronic evidence in another State in a 'rapidly expedited manner' – such as through direct cooperation with service providers in that jurisdiction, and expedited disclosure of data in emergency situations where lives are at risk.
- ☐ Simultaneously, it provides for a system of human rights and rule of law safeguards for such tools, including for the protection of personal data transferred under the Protocol.
- ☐ Relates to specific criminal investigations or proceedings, not only with respect to cybercrime but any criminal offence involving electronic evidence.
- ☐ The effective use and implementation of the provisions of the Protocol
- ☐ shall be periodically assessed by the States.
- ☐ Of particular concern are the challenges of territoriality and jurisdiction related to electronic evidence, given that specified data needed in a criminal investigation may be stored in multiple, shifting or unknown jurisdictions ('in the cloud'),
- ☐ Provides for complementary tools to obtain the disclosure of subscriber data directly from a service provider and to obtain the information from relevant domain name registrars and registries in another State.
- ☐ Refers to emergency situations, where there is a significant and imminent risk to the life or safety of any natural person, by calling upon States to provide for emergency mutual assistance.

77 Ibid. According to the Explanatory report to the Second Additional Protocol to the Convention on Cybercrime, the amending protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data was opened for signature during the drafting of the Protocol on October 2018. The drafting process of the Protocol included Parties not subject, at the time, to Council of Europe instruments on data protection or to European Union data protection rules. Accordingly, significant efforts were undertaken to ensure a balanced Protocol reflective of the many legal systems of States likely to be Parties to the Protocol while respecting the importance of ensuring the protection of privacy and personal data as required by the constitutions and international obligations of other Parties to the Convention.

78 Ibid., p. 38.

3.2. THE EU LAW

Among the legal instruments within the EU, the **Charter of Fundamental Rights of the European Union**,[79] the **human rights directives** and the **EU cooperation instruments** in criminal matters are those that are the most pertinent for the collection, preservation, use, and cross-border exchange of electronic evidence while upholding the presumption of innocence and other associated rights.

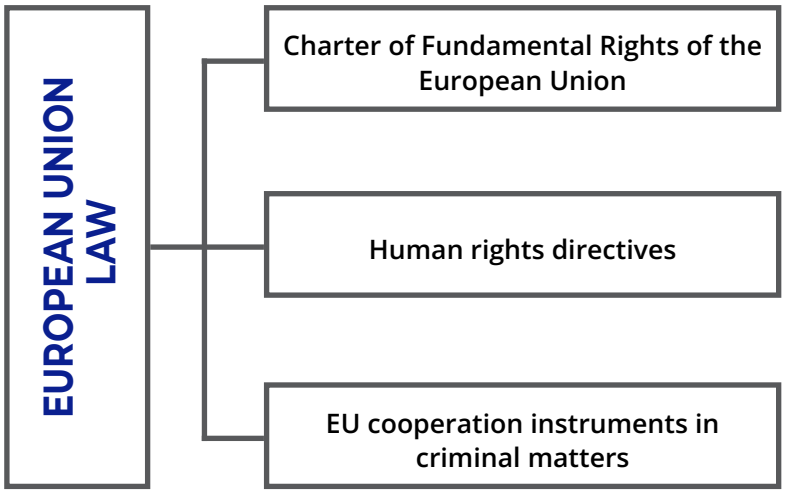

Figure 2: European Union law related to electronic evidence

3.2.1. The Charter of Fundamental Rights of the European Union and the procedural rights directives

Article 2 of the Treaty on European Union (the Treaty of Lisbon)[80] provides that '*The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities*.' These values resonate in the *Charter of Fundamental Rights of the European Union* (the Charter), which, as a legal instrument that has the same value as the Treaties, enshrines the fundamental rights people enjoy in the EU. The Charter applies in conjunction with national and international fundamental rights protection systems, including the European Convention on Human Rights. The Charter has become legally binding on the EU and its Member States with the entry into force of the Treaty of Lisbon, in December 2009.

The Charter encompasses rights and freedoms organised into six titles: dignity, freedoms, equality, solidarity, citizens' rights, and justice. Relevant provisions in the Charter concerning electronic evidence primarily pertain to the judicial system. Specifically, these include the **right to a fair trial** (Article 47), the **presumption of innocence**, and the **right to a defence** (both enshrined in Article 48). Additionally, the Charter addresses the **right to the respect for private and family life** (Article 7) and the **right to the protection of personal data** (Article 8).

79 Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, 18 December 2000 (2000/C 364/01), https://www.refworld.org/docid/3ae6b3b70.html.

80 Consolidated version of the Treaty on European Union, OJ C 326, 26.10.2012, p. 13–390.

According to the Charter, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Individuals charged with an offence are presumed innocent until proven guilty in accordance with the law, and their right to a defence is guaranteed. Everyone has the right to respect for their private and family life, home and communications and the right to the protection of personal data concerning themselves. Such data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning them, and the right to have it rectified. As far as this Toolkit is concerned, the same applies to the Charter as it does to the ECHR: it is centred on the presumption of innocence, with fair trial rights and privacy rights being addressed to a lesser extent.

In 2009, the Council of the EU adopted the **Roadmap for strengthening the procedural rights of suspected or accused persons in criminal proceedings** (the Roadmap).[81] Since then, taking a step-by-step approach, six directives on procedural rights have been adopted based on Article 82(2) of the Treaty on the Functioning of the European Union (TFEU).[82] **The three directives particularly relevant in the context of issues addressed by this Toolkit are the Directive 2012/13/EU on the right to information,[83] the Directive 2013/48/ EU on the right of access to a lawyer in criminal proceedings,[84] and the Directive 2016/343/EU on the strengthening of certain aspects of the presumption of innocence**.[85]

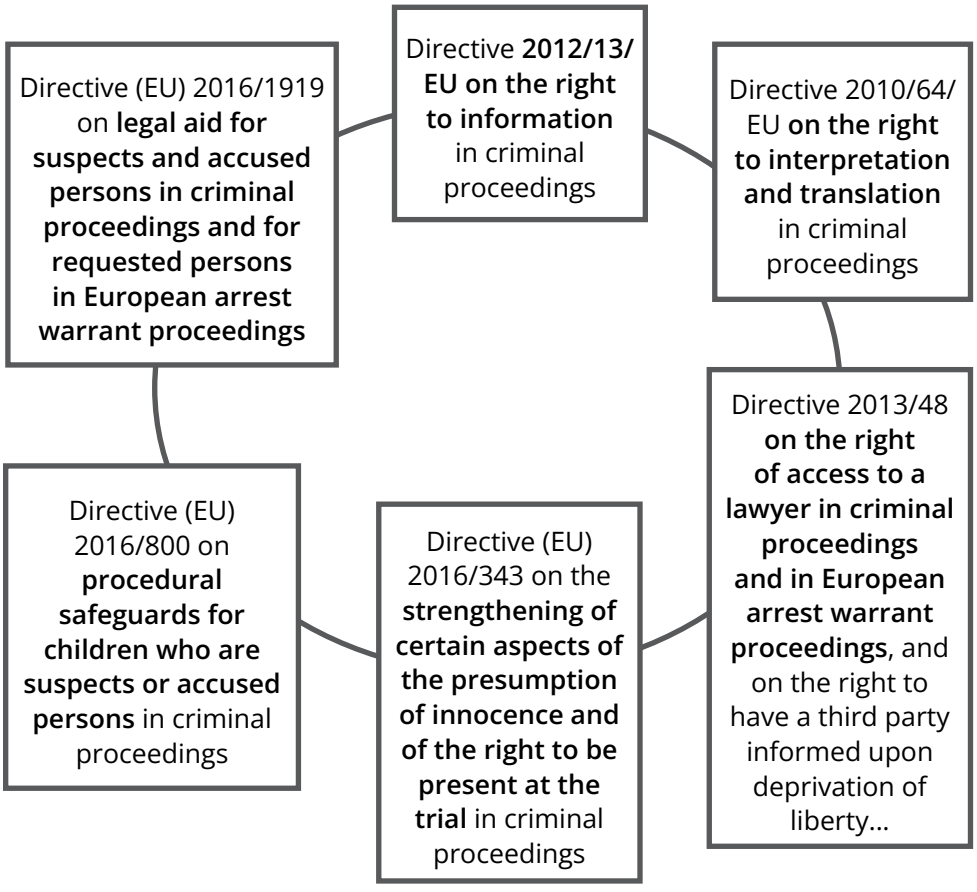

Figure 3: Roadmap directives for strengthening the procedural rights of suspected or accused persons in criminal proceedings

81 Resolution of the Council of 30 November 2009 on a Roadmap for strengthening the procedural rights of suspected or accused persons in criminal proceedings, OJ C 295, 4.12.2009, p. 1–3.

82 Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 47–390.

83 Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, OJ L 142, 1.6.2012, p. 1–10.

84 Directive 2013/48/EU of the European Parliament and o f the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, OJ L 294, 6.11.2013, p. 1–12.

85 Directive 2016/343/EU of the European Parliament and o f the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, OJ L 65, 11.3.2016, p. 1–11.

Directive 2012/13/EU lays down rules concerning the right to information of suspects or accused persons, relating to their rights in criminal proceedings and to the accusation against them. It also lays down rules concerning the right to information of persons subject to a European Arrest Warrant relating to their rights. It applies from the time persons are made aware by the competent authorities of a Member State that they are suspected or accused of having committed a criminal offence until the conclusion of the proceedings, which is understood to mean the final determination of the question of whether the suspect or accused person has committed the criminal offence, including, where applicable, sentencing and the resolution of any appeal. **Member States shall ensure that suspects or accused persons are provided promptly with information concerning (at least) the right of access to a lawyer; any entitlement to free legal advice and the conditions for obtaining such advice; the right to be informed of the accusation; the right to interpretation and translation**; and the right to remain silent. The information shall be given orally or in writing, in simple and accessible language, considering any particular needs of vulnerable suspects or vulnerable accused persons. These rights should be provided as they apply under national law and should be exercised effectively.[86]

Directive 2013/48/EU lays down minimum rules concerning the right of access to a lawyer in criminal proceedings and in proceedings for the execution of a European arrest warrant and the surrender procedures between Member States and the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty. According to this Directive, **Member States should ensure that suspects or accused persons have the right of access to a lawyer without undue delay. In any event, suspects or accused persons should be granted access to a lawyer during criminal proceedings before a court, if they have not waived that right**. The Directive should be implemented considering the provisions of Directive 2012/13/EU, which provide that suspects or accused persons are provided promptly with information concerning the right of access to a lawyer. It applies to suspects or accused persons in criminal proceedings from the time when they are made aware by the competent authorities of a Member State, by official notification or otherwise, that they are suspected or accused of having committed a criminal offence, and irrespective of whether they are deprived of liberty. It applies until the conclusion of the proceedings.[87]

The purpose of the *Directive (EU) 2016/343* is to enhance the right to a fair trial in criminal proceedings by laying down common minimum rules concerning certain aspects of the presumption of innocence and the right to be present at the trial**. In line with the Directive, Member States shall ensure that suspects and accused persons in criminal proceedings are presumed innocent until proved guilty according to law**. Applying to natural persons, the Directive has broader temporal scope than the previous Roadmap directives, which may only commence from when the suspect/accused is informed that they are suspected or accused. **It applies at all stages of the criminal proceedings, from the moment when a person is suspected or accused of having committed a criminal offence, or an alleged criminal offence, until the decision on the final determination of whether that person has committed the criminal offence concerned has become definitive**. It is worth noting that this Directive should apply only to criminal proceedings as interpreted by the Court of Justice of the European Union (CJEU), without prejudice to the case law of the European Court of Human Rights.[88]

86 Directive 2012/13/EU, Articles 1-3.

87 Directive 2013/48/EU, Articles 1-4.

88 Directive (EU) 2013/48, Articles 1-3.

3.2.2. The EU cooperation instruments in criminal matters

Over the last two decades, the EU legal framework in the area of cross-border cooperation in criminal matters has consisted of documents such as **Directive 2014/41/EU regarding the European Investigation Order in criminal matters; the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union; Council Decision 2002/187/JHA setting up Eurojust; Regulation (EU) 2016/794 on Europol; Council Framework Decision 2002/465/JHA on joint investigation teams; and bilateral agreements between the Union and non-EU countries**, such as the Agreement on Mutual Legal Assistance between the EU and the US and the Agreement on MLA between the EU and Japan.

Supplementing the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters and its 1978 Protocol, the *Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union*[89] (EU MLA Convention) entered into force on 23 August 2005. **It aims to encourage and facilitate mutual assistance between judicial, police and customs authorities on criminal matters and to improve the speed and efficiency of judicial cooperation. In line with the Convention, EU countries may share information regarding criminal offences (and administrative infringements) whose punishment or handling is the responsibility of the receiving authority either spontaneously or through requests for mutual assistance**. Requests must be made in writing, transmitted and carried out directly by the national judicial authorities. The EU country requested to provide mutual assistance (requested country) must comply with the formalities and procedures specified by the EU country which made the request (requesting country) and must carry out the request as soon as possible, taking as full account as possible of the deadlines indicated. A judicial authority or a central authority in one EU country may make direct contact with a police or customs authority from another EU country or, in respect of requests for mutual assistance in relation to proceedings, with an administrative authority from another EU country. However, countries may refuse to apply this clause or apply it only under certain conditions. Among various forms of mutual assistance, the Convention explicitly addresses the possibility of cross-border access to and exchange of electronic evidence through interception of telecommunications. Interception may be carried out if requested by a competent authority from another EU country, which is designated to do so in that EU country. Communications may either be intercepted and transmitted directly to the requesting country or recorded for later transmission.[90]

In the decade following the adoption of the Convention, the Mutual Legal Assistance's (MLA) approach to cross-border cooperation in criminal matters, which relied on traditional mutual legal assistance requests, was replaced by the mutual recognition approach. Adopted in April 2014, *Directive 2014/41/EU regarding the European Investigation Order in criminal matters*[91] ('EIO Directive') creates a single comprehensive framework for obtaining evidence through the European Investigation Order (EIO) issued in or validated by the judicial authority in one EU Member State to have investigative measures to gather or use evidence in criminal matters carried out in another EU Member State. **The investigative measures which can be implemented on the basis of EIO include, for instance, the hearing of witnesses, telephone interceptions, covert investigations and information on banking operations.**

89 Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000, p. 3–23.

90 Summaries of EU legislation, Mutual assistance in criminal matters between EU countries, https://eur-lex.europa.eu/EN/legal-content/summary/mutual-assistance-in-criminal-matters-between-eu-countries.html.

91 Directive 2014/41/EU of the European Parliament and f the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, p. 1–36.

The EIO is based on mutual recognition, which means that there are both limited possibilities for refusal by the executing State, and that the executing authority is, in principle, obliged to recognise and ensure execution of the request of the other country. In aggregate, **the EIO offers judicial authorities a simpler and faster alternative to the traditional instruments for requesting evidence by outlining strict deadlines and providing practitioners with a single standard form for obtaining evidence. Across the entire life cycle of the EIO, from drafting to the execution phase, the national authorities are supported by the Eurojust regulation**.[92] Although the EIO Directive does not specifically refer to electronic evidence, due to its wide scope, it constitutes among LEAs and prosecution services the instrument of first choice for a cross-border exchange of electronic evidence in the EU.

Considering that among EU Member States there were no common rules or minimum standard on preserving, collecting and storing of electronic evidence, as well as the admissibility of electronic evidence, the European Commission launched in the beginning of 2018 a consultation procedure in view of the introduction of a system allowing the prompt judicial cooperation in cross-border criminal matters. It was found that a clear and more harmonised framework is desirable to facilitate efficient cooperation in criminal matters and secure fundamental rights. In April 2018, these developments led to the publishing of a draft Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and a draft Directive on laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.

The drafters pointed to the fact that **today, in a growing number of criminal cases, social media, webmail, messaging services and applications are often the only place where investigators can find leads to determine who committed a crime and obtain evidence that can be used in court.** Due to the borderless nature of the internet, such services can be provided from anywhere in the world and do not necessarily require physical infrastructure and a specific location for the storage of data. As a result, in several cases data and evidence is stored outside the country and/or by service providers in other Member States or third countries.[93]

At the same time, the drafters warned that **mechanisms for cooperation between countries, which were developed several decades ago, despite regular reforms proved unable to satisfy the growing need for timely cross-border access to electronic evidence.** They pointed out that in response several Member States and third countries have resorted to expanding their national tools and that this resulted in fragmentation and generation of legal uncertainty and conflicting obligations and raised questions about the protection of fundamental rights and procedural safeguards for suspected and accused persons. Hence, the drafters followed the European Council's call for concrete action based on a common EU approach to make mutual legal assistance more efficient and to improve cooperation between Member State authorities and service providers based in non-EU countries.[94]

Finally, **Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings[95] and Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in**

92 For more information on EIO see Report on Eurojust's casework in the field of the European Investigation Order (Eurojust report), Criminal justice across borders, Eurojust, November 2022. See also Section 6 of this Toolkit.

93 See Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Explanatory memorandum, Council of Europe, Strasbourg, 17 April 2018.

94 Ibid. See also G. Forlani: The E-evidence Package: The Happy Ending of a Long Negotiation Saga, Eucrim 2/2023, pp. 174–181.

95 Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, OJ L 191, 28.7.2023, p. 118–180.

criminal proceedings[96] were adopted on 27 July 2023. The new EU e-evidence legislation aims to facilitate and speed up access to electronic evidence used to investigate and prosecute criminal offences, regardless of where the data is located.

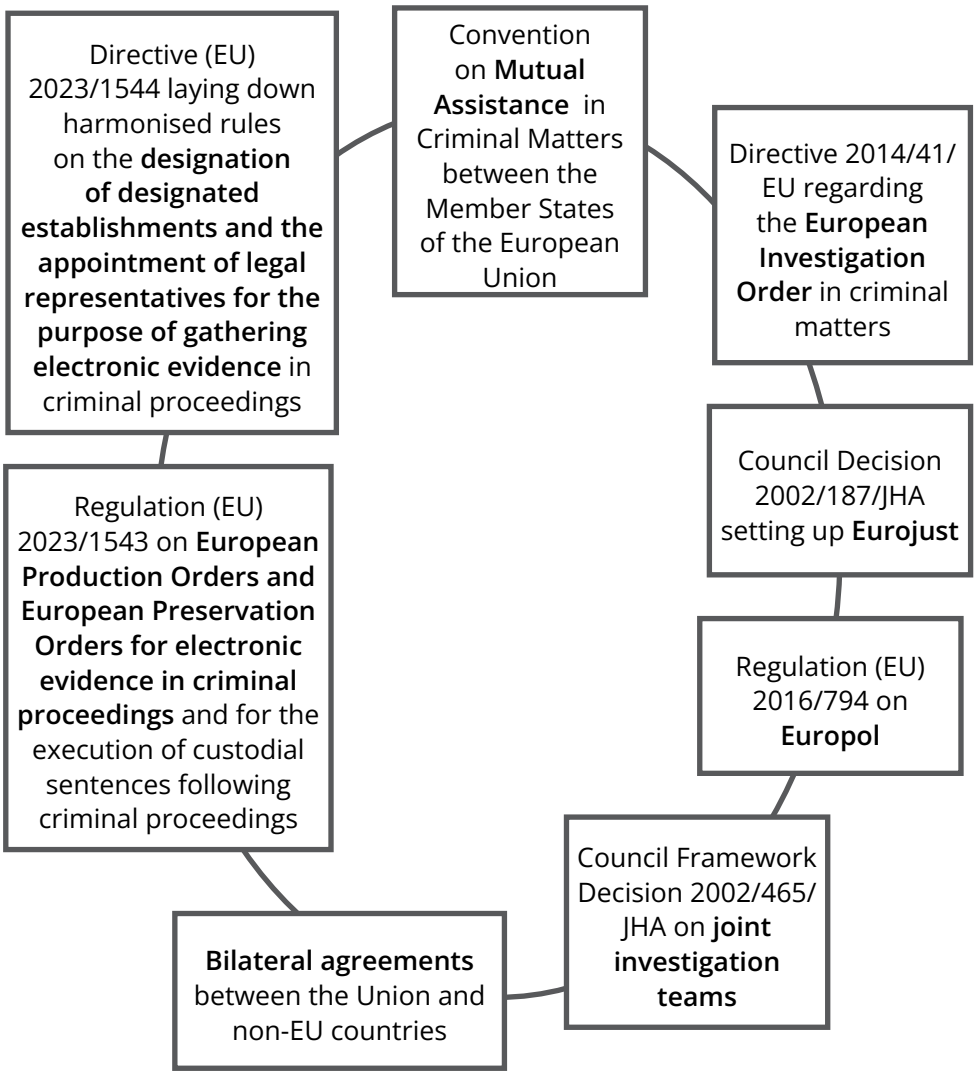

Figure 4: The EU cooperation instruments in criminal proceedings

96 Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, OJ L 191, 28.7.2023, p. 181–190.

3.2.2.1. Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings

Regulation (EU) 2023/1543 aims to facilitate and speed up access to electronic evidence used to investigate and prosecute criminal offences, regardless of where the data is located, through a European Production Order and a European Preservation Order. **The European production order allows an authority (including LEAs under the conditions specified in the Regulation) in one Member State to obtain electronic evidence (such as e-mails, text or messages in-apps, messages, etc.) directly from a service provider, or its legal representative, in another Member State**. If the electronic evidence includes content data or traffic data, except for data requested for the sole purpose of identifying the user, a court or judge must issue or review the order, and the judicial authority must notify the competent authority of the Member State in which the designated establishment is located, or the legal representative resides. This authority of another Member State can stop the production of data in specific circumstances, based on grounds for refusals laid down in the Regulation. **The European preservation order allows a judicial authority in one Member State to request that the designated establishment of a service provider, or its legal representative, in another Member State, preserve specified data prior to a subsequent request to produce the data.**

The Regulation lays down the rules under which an authority of a Member State, in criminal proceedings, may issue a European Production Order or a European Preservation Order and thereby order a service provider offering services in the EU and established in another Member State, or, if not established, represented by a legal representative in another Member State, to produce or to preserve electronic evidence regardless of the location of the data. **The issuing of a European Production Order or of a European Preservation Order may also be requested by a suspect or an accused person, or by a lawyer on that person's behalf within the framework of applicable defence rights**.[97]

Electronic evidence, as referred to in the Regulation, concern data stored by or on behalf of a service provider, in an electronic form, that is used to investigate and prosecute criminal offences. It consists of the following categories of data:[98]

- **subscriber data** (data relating to the subscription to its services pertaining to the identity of a subscriber or customer, such as the provided name, date of birth, postal or geographic address, billing and payment data, telephone number, or e-mail address);
- **data requested for identifying the user** (data such as IP addresses and the relevant source ports and time stamp or technical equivalents of those identifiers and related information for the purpose of identifying the user in a specific criminal investigation);
- **traffic data** (data about service offered by a service provider and generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, data about the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression, and other electronic communications metadata and data, other than

97 Regulation (EU) 2023/1543, Articles 1-2.

98 Regulation (EU) 2023/1543, Article 3.

subscriber data, relating to the commencement and termination of a user access session to a service, such as the date and time of use, the log-in to and log-off from the service); and

– **content data** (data in a digital format, such as text, voice, videos, images and sound, other than subscriber data or traffic data).

The Regulation specifically pertains to stored data, excluding real-time interception of telecommunications (special investigation measures, such as secret surveillance and wiretapping, are not covered by the Regulation).

According to the Regulation,[99] a **European Production Order to obtain subscriber data or data for identifying the user** may be issued only by a judge, an investigating judge, a public prosecutor or an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. In the latter case, the order shall be validated, after examination of its conformity with the conditions for issuing a European Production Order under the Regulation, by a judge, a court, an investigating judge or a public prosecutor in the issuing State.

In contrast, a **European Production Order to obtain traffic or content data** may be issued only by a judge, an investigating judge or an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. In the latter case, the order shall be validated, after examination of its conformity with the conditions for issuing a European Production Order under the Regulation, by a judge, a court or an investigating judge in the issuing State.

A **European Preservation Order for data of any category** may be issued by a judge, an investigating judge, a public prosecutor or an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. In the latter case, the order shall be validated, after examination of its conformity with the conditions for issuing a European Preservation Order under the Regulation, by a judge, a court, an investigating judge or a public prosecutor in the issuing State.

In an **emergency case**, the competent authorities may exceptionally issue a European Production Order for subscriber data or identification data without prior validation of the order, where validation cannot be obtained in time and where those authorities could issue an order in a similar domestic case without prior validation. However, the issuing authority shall seek *ex-post* validation of the order concerned without undue delay.[100]

Article 5 of the Regulation provides for the **conditions for issuing a European Production Order**. A European Production Order shall be necessary for and proportionate to the purpose of the proceedings, considering the rights of the suspect or the accused person, and may only be issued if a similar order could have been issued under the same conditions in a similar domestic case. In addition to the general condition, the Regulation sets out **different specific conditions for issuing a European Production Order to obtain subscriber data or identification data on the one hand, and traffic data and content data on the other**. The same article also provides for the information which should be included in a European Production Order. While a European Production Order shall be addressed to the service provider acting as controller in accordance with Regulation (EU) 2016/679 on the protection of natural persons regarding the processing of personal data, by way of exception, it may be directly addressed to the service provider that stores or otherwise processes

99 Ibid., Article 4, para. 1–2.
100 Ibid., para. 3.

the data on behalf of the controller. The conditions for issuing a European Preservation Order are enshrined in Article 6.

European Production Order			
Type of data	**Issuing & validation authority**	**General conditions for issuing**	**Specific conditions for issuing**
Subscriber data or data for identifying the user	Judge, investigating judge, public prosecutor or law enforcement agency (with prior validation by judge, court, investigating judge or public prosecutor) **In an emergency case, prior validation not needed where it cannot be obtained on time and where LEA could issue an order in a similar domestic case without prior validation	If necessary for and proportionate to the purpose of the proceedings If a similar order could have been issued under the same conditions in a similar domestic case Rights of the suspect or the accused person should be considered	For all criminal offences For execution of a custodial sentence or a detention order of at least 4 months, imposed by a decision that was not rendered in absentia, where the person convicted absconded from justice
Traffic or content data	Judge, investigating judge or law enforcement agency (with prior validation by judge, court or investigating judge)		For criminal offences punishable in the issuing State by a custodial sentence by a maximum period of at least 3 years For criminal offences as defined in Articles 3 to 12 and 14 of Directive (EU) 2017/541 For offences as defined in EU directives determined by Regulation (Art. 5), if they are wholly or partly committed by means of an information system For the execution of a custodial sentence or a detention order of at least 4 months, imposed by a decision that was not rendered in absentia, in cases where the person convicted absconded from justice, for specific criminal offences referred to in Regulation

Table 1: European Production Order

European Preservation Order			
Type of data	**Issuing or validation authority**	**General conditions for issuing**	**Specific conditions for issuing**
Data of any category	Judge, investigating judge, public prosecutor or law enforcement agency (with prior validation by judge, court, investigating judge or public prosecutor)	If necessary for and proportionate to the purpose of preventing the removal, deletion or alteration of data with a view to issuing a subsequent request for production of those data via MLA, an EIO or an EPO For all criminal offences, if it could have been issued under the same conditions in a similar domestic case For the execution of a custodial sentence or a detention order of at least 4 months, imposed by a decision that was not rendered in absentia, in cases where the person convicted absconded from justice Rights of the suspect or the accused person should be considered	None

Table 2: European Preservation Order

The Regulation also sets up **rules for the notification to the enforcing authority where a European Production Order is issued to obtain traffic data or content data**.[101] The issuing authority shall notify the enforcing authority by transmitting the European Production Order Certificate (see below) to that authority at the same time as it transmits such certificate to the addressee. This applies only if, at the time of issuing the order, the issuing authority has reasonable grounds to believe that (a) the offence has been committed, is being committed or is likely to be committed in the issuing State, and (b) the person whose data are requested resides in the issuing State. The notification is not required where a European Production Order is issued to obtain subscriber data and identification data.

According to Article 9 of the Regulation, a **European Production Order or a European Preservation Order shall be transmitted to the addressee through a European Production Order Certificate (EPOC) or through a European Preservation Order Certificate (EPOC-PR)**. Upon receipt of an EPOC, the addressee shall act expeditiously to preserve the data requested. Regarding the execution, different regimes apply to an EPOC where a notification to the enforcing authority is required and where it is not and in emergency cases.[102] A special regime is set out for the execution of an EPOC-PR.[103]

101 Ibid., Article 8.
102 Ibid., Article 10.
103 Ibid., Article 11.

The issuing authority or, where applicable, the validating authority shall complete the EPOC or EPOC-PR set out in Annexes I and II to the Regulation. An EPOC or EPOC-PR shall contain the information listed in Article 5. **When an EPOC is received, the requested data must be transmitted directly to the issuing authority or the law enforcement authorities within 10 days, or in cases of emergency within 8 hours. In cases where a notification is required, the enforcing authority has 96 hours to raise a ground for refusal**. When an EPOC-PR is received, the data requested must be preserved without delay for a period of 60 days (which can be extended for another 30 days by the issuing authority), unless there has been a subsequent request for the data to be produced. If preserving the data is no longer necessary, the issuing authority must inform the addressee without delay. The issuing authority has 5 days to provide clarification or correction when the addressee cannot comply with the order because it is incomplete or contains manifest errors. The addressee must contact the issuing authority without undue delay if they cannot comply because of factors beyond their control, notably where the person whose data is requested is not their customer, or the data has been deleted before receiving the order. The issuing authority must inform the person whose data is being requested without undue delay. Service providers must ensure the confidentiality, secrecy and integrity of the EPOC or the EPOC-PR and of the data produced or preserved.[104]

Grounds for refusal of European Production Orders are enshrined in Article 12 of the Regulation. Where the issuing authority has notified the enforcing authority pursuant to the provisions of the Regulation, the enforcing authority shall, as soon as possible but at the latest within 10 days following receipt of the notification, or, in emergency cases, at the latest within 96 hours following such receipt, assess the information set out in the order and, where appropriate, raise one or more of the following grounds for refusal: (a) the data requested are protected by immunities or privileges granted under the law of the enforcing State; (b) in exceptional situations if the execution of the order would entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and in the Charter; (c) the execution of the order would be contrary to the principle of *ne bis in idem*; and (d) the conduct for which the order has been issued does not constitute an offence under the law of the enforcing State. Where the enforcing authority raises a ground for refusal pursuant to paragraph 1, it shall inform the addressee and the issuing authority. The addressee shall stop the execution of the European Production Order and not transfer the data, and the issuing authority shall withdraw the order. However, before deciding to raise a ground for refusal, the enforcing authority shall contact the issuing authority by any appropriate means, to discuss the appropriate measures to take.

Member States shall lay **down rules on pecuniary penalties applicable to infringements of Articles on the execution of an EPOC and an EPOC-PR** and shall take all measures necessary to ensure that they are implemented. They must ensure, *inter alia*, that pecuniary penalties of up to 2% of the service provider's total worldwide annual turnover can be imposed. Service providers are not held liable in Member States for any prejudice to their users or third parties exclusively resulting from compliance with an EPOC or an EPOC-PR in good faith.[105]

Procedure for enforcement where the addressee does not comply with an EPOC within the deadline or with an EPOC-PR, without providing reasons accepted by the issuing authority, and where the enforcing authority has

104 Ibid., Articles 9–11.
105 Ibid., Article 15.

not invoked any of the grounds for refusal (if applicable), is laid down in Article 16 of the Regulation.

Individuals whose data were requested via a European Production Order shall have the **right to effective remedies against such order**, including during criminal proceedings in which the data were being used.

The Regulation applies from 18 August 2026.

3.2.2.2. Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives

Directive (EU) 2023/1544, the other piece of the new EU e-evidence law, **obliges all service providers offering services in the EU to designate an establishment or appoint a legal representative to be responsible for receiving, complying with and enforcing decisions and orders (including the European Production and Preservation Orders) issued by competent authorities of Member States to gather evidence in criminal proceedings**. The objective is to ensure that all service providers operating in the EU have the same obligations regarding access to electronic evidence. Member States must ensure that:[106] service providers (a) established in the EU specify a designated establishment and service providers (b) not established in the EU appoint a legal representative;

- addressees are established or reside in a Member State where the service providers offer their services;
- addressees can be subject to enforcement procedures;
- the decisions and orders issued by the competent authorities for gathering evidence in criminal proceedings are addressed to the designated establishment or legal representative;
- service providers give their designated establishments and legal representatives the necessary powers and resources to comply;
- the designated establishment, the legal representative, and the service provider can be held jointly and severally liable for non-compliance and may be subject to penalties;
- establishments or legal representatives need to be designated within 6
- months of the legislation being transposed into national law;
- each service provider supplies their respective contact details and any changes, in writing, to the central authority of the Member State where its designated establishment is located or where its legal representative resides.

Member States must set out rules on effective, proportionate and dissuasive penalties to be applied to infringements of national laws adopted under the directive and take all measures necessary to ensure that they are implemented. They must notify the European Commission of these rules and any subsequent amendments. They must also inform the Commission annually about non-compliant service providers, relevant enforcement action taken against them, and the penalties imposed. Finally,

106 Electronic evidence in criminal proceedings – designated establishments and legal representatives of service providers, Summaries of EU Legislation, https://eur-lex.europa.eu/EN/legal-content/summary/electronic-evidence-in-criminal-proceedings-designated-establishments-and-legal-representatives-of-service-providers.html.

Member States must designate one or more central authorities to ensure that the directive is applied consistently and proportionately. The central authorities coordinate and cooperate with each other and where relevant with the Commission, and provide any appropriate information and assistance to each other, particularly on enforcement actions.[107]

The directive must be transposed into national law by 18 February 2026.

In Section 6.3 of this Toolkit, Regulation (EU) 2023/154 and Directive (EU) 2023/1544 will be examined from a practical standpoint.

CHECKLIST OF KEY POINTS ON THE 'EU E-EVIDENCE PACKAGE'

- ☐ Adopted on 27 July 2023, Regulation (EU) 2023/1543 and Directive (EU) 2023/1544 are EU legal instruments aiming at improving cross-border access to e-evidence in judicial proceedings. The so-called 'e-evidence package' aims to facilitate and speed up access to electronic evidence used to investigate and prosecute criminal offences, regardless of the location of the data, through a European Production Order and a European Preservation Order.
- ☐ All service providers offering services in the EU must designate an establishment or appoint a legal representative to be responsible for receiving, complying with and enforcing the European Production and Preservation Orders. While service providers established in the EU shall specify a designated establishment, service providers not established in the EU shall appoint a legal representative.
- ☐ The European production order and the European Preservation Order allow an authority (including LEAs under the conditions specified in the Regulation) in one Member State to obtain electronic evidence directly from a service provider, or its designated establishment or legal representative, in another Member State, and to request that the designated establishment of a service provider, or its legal representative, in another Member State preserve specified data prior to a subsequent request to produce the data.
- ☐ If the electronic evidence includes content data or traffic data, except for data requested for the sole purpose of identifying the user, a court or judge must issue or validate the order, and the judicial authority must notify the competent authority of the Member State in which the designated establishment is located, or the legal representative resides. This authority of another Member State can stop the production of data in specific circumstances, based on grounds for refusals laid down in the Regulation.
- ☐ European production or preservation orders are transmitted through a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR). When an EPOC is received, the requested data must be transmitted directly to the issuing authority or the LEAs within 10 days, or in cases of emergency within 8 hours. In cases where a notification is required, the enforcing authority has 96 hours to raise a ground for refusal.

107 Ibid.

4. THE PRESUMPTION OF INNOCENCE AND FAIR TRIAL RIGHTS

Enshrined in all the most important European and international treaties and covenants, the **presumption of innocence** is a fundamental tenet affirming that a suspect or an accused individual is to be considered innocent until proven guilty. This principle, deeply embedded in legal traditions worldwide, serves as a bedrock for fair trial rights, such as the right to information in criminal proceedings, the right to access legal assistance and to sufficient time and resources for defence preparation, the right to remain silent, the right against self-incrimination and protection against false confession, and the right to an impartial and independent tribunal.

The presumption of innocence is a **fundamental right and key principle at the heart of fair trial rights protection** under Article 6 of the ECHR and Article 48 of the European Charter, as well as under the provisions of the International Covenant on Civil and Political Rights, the Universal Declaration of Human Rights, and several other international treaties and covenants. It is also a principle or a rule in the constitutions of the EU Member states and other modern democratic countries, including those participating in the INNOCENT project.[108]

The ECHR, for example, in the second paragraph of Article 6, which determines the right to a fair trial, stipulates that '***Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law***.' An identical provision can be found in Article 14 of the International Covenant on Civil and Political Rights. Similarly, but broadly, the presumption of innocence is defined by Article 11 of the Universal Declaration of Human Rights: '*Everyone charged with a penal offence has the right to be presumed innocent until proved guilty according to law in a public trial at which he has had all the guarantees necessary for his defence*.' In EU law, the presumption is defined by Article 48 of the Charter and more particularly by Directive (EU) 2016/343.

In the text of the ECHR, the word 'accused' may be misleading because it can falsely imply that the presumption of innocence only applies after the formal initiation of further proceedings. According to the ECtHR, the presumption applies before the formal initiation of the proceedings, if certain actions of the LEAs have the same effects as if the person had already been accused. In other words, the presumption applies not from the moment the criminal charge is filed, but from the moment the person's position is significantly affected.[109] The latter also follows from Article 2 of Directive (EU) 2016/343, which states that **persons that are presumed innocent until proved guilty according to law are accused persons as well as suspects.**

According to the ECtHR jurisprudence, the presumption of innocence concerns the following rights and safeguards: **prohibition of the use of compulsion, the right to remain silent, the right to not incriminate oneself, the principle that places the burden of proof on the prosecution, the principle that any reasonable doubts on the guilt should benefit the**

108 Interestingly, with the exception of Croatian Constitution, according to the constitutions of other participating countries any person charged with criminal offence shall be presumed innocent until found guilty by a final judgement. In contrast, the Croatian Constitution provides that everyone is presumed innocent and may not be held guilty of a criminal offence until such guilt is proven by – not a final but – a binding court judgment. Whether the different wording in the constitutions of the participating countries consequently means that the legal regulations of these countries also differ in terms of substantive standards for ensuring the presumption of innocence in domestic law is not entirely clear. There is no doubt, however, that uniform minimal standards for all countries and their legal arrangements are determined by the legal mechanisms of the CoE and the EU.

109 See ECtHR, *Imbrioscia v. Swicerland*, a. No 13972/8, judgement of 24 November 1993, para. 36, cited in A. Erbežnik, Z. Dežman: Introduction to Criminal Procedure Law [Uvod v kazesko procesno pravo], GV Založba, Lexpera, Ljubljana, 2022, p. 248.

accused, and the **right to an impartial and independent tribunal**.[110] Additionally, two additional fair trial rights are also inextricably linked to the effective implementation of the presumption of innocence in pre-trial investigation: the **right to information** in criminal proceedings and the right to access to legal assistance and to have adequate time and facilities for the preparation of the defence.

The ECtHR emphasised that the right to remain silent and the privilege against self-incrimination, which are not explicitly mentioned in Article 6, are generally accepted international standards that lie at the heart of the idea of a fair trial in Article 6 of the ECHR and, further to this, that the privilege against self-incrimination in particular presupposes that in a criminal case the prosecution and LEAs are prohibited from obtaining evidence by coercive methods.[111] Particularly noteworthy is that the Court distinguishes between testimonial and non-testimonial evidence, maintaining that the privilege and the right to remain silent do not protect against the use of coercion in obtaining material that is in the defendant's domain independently of their will (e.g. documents, blood, urine and DNA samples, etc.).[112]

In a similar vein, Article 6 of Directive (EU) 2016/343[113] imposed on Member States an obligation to ensure that the burden of proof for establishing the guilt of suspects and accused persons was placed on the prosecution. Moreover, according to Article 7, Member States must ensure that any doubt as to the question of guilt is to benefit the suspect or accused person, including where the court assesses whether or not the person concerned should be acquitted. They must ensure that suspects and accused persons have the right to remain silent in relation to the criminal offence that they are suspected or accused of having committed, and that suspects and accused persons have the right to not incriminate themselves. The exercise by suspects and accused persons of the right to remain silent or of the right to not incriminate oneself shall not be used against them and shall not be evidence that they have committed the criminal offence concerned. However, the **exercise of the right to not incriminate oneself shall not prevent the competent authorities from gathering evidence (a) which may be lawfully obtained with legal powers of compulsion, and (b) which has an existence independent of the will of the suspects or accused persons**. Article 7 of the Directive (EU) 2016/343 also provides that Member States may allow their judicial authorities to consider, when sentencing, cooperative behaviour of suspects and accused persons.

110 Erbežnik, Dežman, op. cit., p. 253. See also the INNOCENT Report, supra, p. 36 and the EU Directive on the Presumption of Innocence: Implementation Toolkit, Legal Experts Advisory Panel, Fair Trials, p. 5, https://www.fairtrials.org/app/uploads/2022/01/Presumption-of-Innocence-Toolkit_2.pdf.

111 See ECtHR, *Saunders v. the United Kingdom,* a. No 19187/91, judgement of 17 December 1996, para. 68 and *Heaney and Meguiness v. Ireland*, a. No 34720/97, judgement of 21 December 2000, para. 40.

112 See ECtHR, *Heaney and Meguiness v. Ireland*, a. No 34720/97, judgement of 21 December 2000, para. 40 and *Zličić v. Serbia*, a. No 73313/17 and 20143/19, judgement of 26 January 2021 (see the partial dissenting opinion of judge Bošnjak).

113 Supra. Directive (EU) 2016/343 was drafted following the European Commission's view that, in practice, the protection of the principle of presumption of innocence by the ECHR and ECtHR has not resulted in sufficient protection of suspects or accused persons in the EU. See the EU Directive on the Presumption of Innocence: Implementation Toolkit, supra, p. 5.

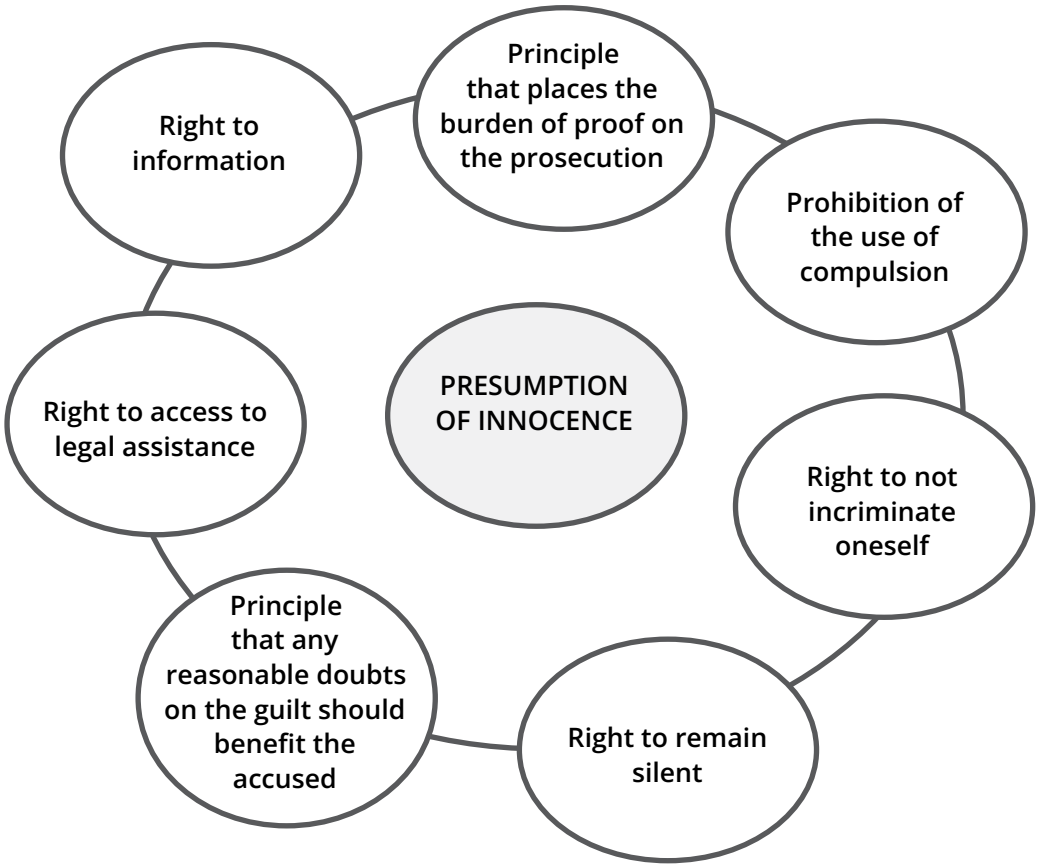

Figure 5: Principles and rights related to the presumption of innocence

This Toolkit delves further into several principles and rights related to the presumption of innocence, including (i) the principle that places the burden of proof on the prosecution, emphasising that any reasonable doubts about guilt should favour the accused; (ii) the right against self-incrimination; (iii) the right to not cooperate; (iv) the right to remain silent; (v) the right to information in criminal proceedings; and (vi) the right to access legal assistance, along with the entitlement to sufficient time and resources for defence preparation. The implications of these facets of the presumption of innocence for the collection, preservation, use, and exchange of electronic evidence are explored in Section 6.

4.1. THE PRINCIPLE THAT PLACES THE BURDEN OF PROOF ON THE PROSECUTION

Under Article 6 of Directive (EU) 2016/343, **Member States are required** '***to ensure that the burden of proof for establishing the guilt of suspects and accused persons is on the prosecution***'. It further states that '***[t]his shall be without prejudice to any obligation on the judge or the competent court to seek both inculpatory and exculpatory evidence, and to the right of the defence to submit evidence in accordance with the applicable national law***.' Lastly, Article 6(2) of the Directive provides that **any doubt as to the question of guilt**

is to benefit the suspect or accused person, including where the court assesses whether the person concerned should be acquitted.[114]

The Directive reflects the ECtHR, which in *Barberà, Messegué and Jabardo v Spain* held that Article 6(2) ECHR requires, *inter alia*, that the burden of proof is on the prosecution, and any doubt should benefit the accused.[115] In *Salabiaku v. France*, the ECtHR has further explained that **the fact that the burden of proof is on the prosecution implies the right of the defence to submit evidence**. According to the ECtHR, the principle requires that **it is for the prosecution to inform the accused of the case that will be made against them**, so that they may prepare and present their defence accordingly, and to adduce evidence sufficient to convict them.[116]

As the Directive, **the ECtHR has not taken this to be an absolute principle**. On the contrary, it permits the application of legal presumptions of fact or of law. Such presumptions should be applied with due respect for the rights of the defence in any event and considering the importance of what it is at stake. This means that when applying presumptions of fact and law, Member States must consider whether the means employed are reasonably proportionate to the legitimate aim sought to be achieved. For example, in the case of *Salabiaku v France*, the Court established that the **evidential burden may be shifted to the defence but the importance of what is at stake and the safeguards which exist to protect the rights of the defence must be considered when determining whether a reverse burden is acceptable**.[117]

4.2. THE RIGHT TO REMAIN SILENT, THE RIGHT TO NOT COOPERATE AND THE RIGHT TO NOT INCRIMINATE ONESELF

Article 7 of Directive (EU) 2016/343 requires Member States to ensure that suspects and accused persons have the right to remain silent and the right to not incriminate themselves in relation to the criminal offence that they are suspected or accused of having committed. As confirmed in Recital 5 of the Directive, during interrogations, individuals should not be forced to produce incriminating information, evidence, or documents. In essence, this provision protects the freedom of a suspect and accused persons to choose whether to cooperate with the authorities, (i.e. whether to speak or to remain silent when questioned).[118]

The Directive codifies the approach of the ECtHR and states clearly that the right to remain silent and to not incriminate oneself are essential elements of the right to be presumed innocent until proven guilty. In *Saunders v the United Kingdom*, the ECtHR stated that the **rationale of these rights lies, *inter alia*, in the protection of the accused against improper compulsion by the authorities, thereby contributing to the avoidance of miscarriages of justice**. Following this rationale, other criminal procedural rights, such as the **right of access to a lawyer and the right to information, are intended to bolster the protection of the rights to remain silent and to not incriminate oneself**. Suspects and accused persons must promptly be informed of their right to remain silent and of their right to access a lawyer, so that the latter can help such suspects and accused to understand and exercise their right to remain silent.[119]

114 EU Directive on the Presumption of Innocence: Implementation Toolkit, supra, p. 21.

115 ECtHR, Barberà, Messegué and *Jabardo v. Spain*, a. No 10590/83, judgement of 6 December 1988, para. 77. See also the EU Directive on the Presumption of Innocence: Implementation Toolkit, supra, p. 22.

116 See the EU Directive on the Presumption of Innocence: Implementation Toolkit, supra, ibid.

117 ECtHR, *Salabiaku v. France*, a. No 10519/83, judgement of 7 October 1988.

118 EU Directive on the Presumption of Innocence: Implementation Toolkit, supra, p. 24.

119 Ibid. p. 24–25.

Importantly, ECtHR stated in *Allan v. the United Kingdom* that **the scope of the right to remain silent and to not incriminate oneself is not confined to cases where duress has been brought to bear on the accused** or where the will of the accused has been directly overborne in some way. **Instead, these two rights imply the freedom of a suspect or accused person to choose whether they wish to answer questions or give statements. This freedom of choice is undermined when a suspect has decided to remain silent, and the authorities use deceitful tactics to influence them to make a confession or any other statements of an incriminatory nature** which they were unable to obtain during questioning.[120]

According to Article 7(3) of the Directive, the **exercise of the right to not incriminate oneself is without prejudice to any acts from the competent authorities directed to gather evidence that has been lawfully obtained with *legal powers of compulsion* and which existed *irrespective of the will of the suspects or accused persons***. Under Recital 29 of the Directive, this includes materials acquired pursuant to a warrant, materials in respect of which there is a legal obligation of retention, and production upon request of breath, blood or urine samples and bodily tissue for the purpose of DNA testing.[121]

As regards to the limits of illegitimate use and degree of compulsion, it is necessary to turn to the jurisprudence of the ECtHR. In *Jalloh v Germany*, the Court established that to determine whether the applicant's right to not incriminate themselves has been violated, the Court will have regard to the following factors:

a. the nature and degree of compulsion used to obtain the evidence;
b. the weight of the public interest in the investigation and punishment of the offence in issue;
c. the existence of any relevant safeguards in the procedure; and
d. the use to which any material so obtained is put.[122]

As a rule, the **ECtHR has established that the use of compulsory powers in obtaining evidence is justified by the public interest in prosecuting crime, provided it does not violate certain other rights such as the prohibition of inhuman and degrading treatment and torture** under Article 3 of the ECHR. More precisely, according to the ECtHR, the use of any evidence obtained in breach of the prohibition of torture from Article 3 of the ECHR will render the proceedings unfair.[123]

Weighting the public interest in the investigation and punishment of the offence, the ECtHR held that the decision to administer emetics into the body of the accused by force was disproportionate and could not be justified when considering that it targeted a street dealer who was offering drugs for sale on a comparatively small scale and who was eventually given a 6-month suspended prison sentence and probation.[124] However, according to the ECtHR, the public interest cannot be invoked to justify the use of answers compulsorily obtained in a non-judicial investigation to incriminate the accused during the trial proceedings.[125] The security and public order concerns also cannot justify a provision which extinguishes the very essence of the applicants' rights to silence and against self-incrimination.[126]

Regarding the existence of relevant safeguards in the procedure, in *Salduz v. Turkey,* the ECtHR noted early access to a lawyer is part of the procedural safeguards to which the ECtHR will have particular regard when examining

120 ECtHR, *Allan v. the United Kingdom*, a. No 48539/99, judgement of 28 August 2001, para. 50. See also the EU Directive on the Presumption of Innocence: Implementation Toolkit, supra, p. 26.

121 EU Directive on the Presumption of Innocence: Implementation Toolkit, supra, p. 27.

122 ECtHR, Jalloh v Germany, a. No 54810/00, judgement of 11 July 2006, para. 117. See also the EU Directive on the Presumption of Innocence: Implementation Toolkit, supra, p. 27–28.

123 Jalloh v Germany, para. 119. See also the EU Directive on the Presumption of Innocence: Implementation Toolkit, supra, p. 28.

124 Jalloh v Germany, ibid.

125 Saunders v. the United Kingdom, para. 74. See also the EU Directive on the Presumption of Innocence: Implementation Toolkit, supra, p. 29.

126 Heaney and Mcguinness v. Ireland, para. 58. See also the EU Directive on the Presumption of Innocence: Implementation Toolkit, supra, ibid.

whether a procedure has extinguished the very essence of the privilege against self-incrimination.[127]

Article 7(4) of the Directive establishes that **Member States may allow their judicial authorities to consider cooperative behaviour of suspects and accused persons when sentencing**. This somewhat ambiguous provision raises concerns because it could be misused to incite suspects and accused persons to waive their right to silence and right to not incriminate themselves in exchange for a shorter sentence. Moreover, it is possible that this provision could be misunderstood as justifying lengthier sentences where someone has simply exercised their right to silence.[128] Section 6.1 of this Toolkit will highlight that, in practice, the implementation of this provision raises specific concerns, particularly concerning the collection and use of electronic evidence.

Article 7(5) of the Directive implies that **the fact that a suspect or accused person has asserted their right to remain silent or the right to not incriminate themselves should not be used against them and should not, in itself, be evidence that the person concerned has committed the criminal offence concerned**. However, following Recital 28 of the Directive, the prohibition established **in this Article does not preclude the possibility of judges taking into account the silence of the accused to evaluate other evidence or for the purpose of sentencing, provided that, in doing so, the proceedings remain fair for the defendant**.[129] A similar approach can be found in *Murray v. the United Kingdom*.[130] According to the ECtHR, the drawing of negative inferences from the accused's silence is not incompatible with Article 6 of the ECHR, provided that judicial safeguards operate to ensure fairness. Where prosecution establishes *prima facie* that the accused has committed an offence, it is then permissible for a court to draw an inference of guilt from the accused's failure to provide an explanation exclusively where this is the only common-sense assumption to be made. Article 7(5) and the corresponding approach of the ECtHR raises concerns regarding the collection and use of electronic evidence and will, therefore, be discussed in Section 6.1.

4.3. THE RIGHT TO INFORMATION IN CRIMINAL PROCEEDINGS

The right to information about procedural rights in criminal proceedings originates from Articles 5 and 6 of the ECHR and Articles 6, 47 and 48 of the Charter. **Article 6(3)(a) of the ECHR specifically lists the right to information about the accusation as a minimum safeguard in criminal proceedings, while Article 5(2) provides for the right of arrested persons to be informed of the reasons for their arrest and any charges against them. Although the ECHR does not specifically set out the right to information about procedural rights, the ECtHR ruled that authorities must ensure that the accused have sufficient knowledge of their right to legal assistance and legal aid, and of their right to remain silent and not incriminate themselves**.[131]

Building on the general rights established in Articles 47 and 48 of the Charter, **Directive 2012/13/EU on the right to information in criminal proceedings contains rules on the right to information about: procedural**

127 ECtHR, *Salduz v. Turkey*, a. No 36391/02, judgement of 27 November 2008, para. 54. See also the EU Directive on the Presumption of Innocence: Implementation Toolkit, supra, ibid.

128 The EU Directive on the Presumption of Innocence: Implementation Toolkit, supra, p. 29.

129 Ibid.

130 ECtHR, *John Murray v. the United Kingdom*, a. No 18731/81, judgement of 8 February 1996, paras. 41–58.

131 Rights in practice: right to access to a lawyer and procedural rights in criminal and European arrest warrant proceedings, European Union Agency for Fundamental Rights, 2019, p. 24, http://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-rights-in-practice-access-to-a-lawyer-and-procedural-rights-in-criminal-and-european-arrest-warrant-proceedings.pdf. The European Union Agency for Fundamental Rights (FRA) refers to the following ECtHR's cases: *Padalov v. Bulgaria*, a. No 54784/00, judgement of 10 November 2006, para. 54; *Aleksandr Zaichenko v. Russia*, a. No 39660/02, judgement of 18 February 2010, para. 38; *Panovits v. Cyprus*, a. No 4268/04, judgement of 11 December 2008, paras. 65 and 72.

rights; the accusation; the reasons for detention for persons deprived of liberty; the right to access a lawyer; the right to interpretation and translation; and the right to remain silent and to not incriminate themselves. The Directive provides, in Article 3(2) and Article 4, that information about rights should be given orally or in writing, in simple and accessible language, considering any needs of vulnerable defendants. **Only when defendants are deprived of liberty do the relevant authorities have to provide them with a written 'letter of rights', drafted in simple and accessible language so that it can be easily understood by a layperson** without any knowledge of criminal procedural law. Accordingly, the directive stresses the need for people to understand the information provided.[132] Relevant case law of the ECtHR also establishes requirements of accessibility of information, as only a defendant's effective understanding of rights makes it possible for him or her to exercise those rights.

According to the European Union Agency for Fundamental Rights (FRA), in practice, authorities in EU Member States that are covered by their report (Austria, Bulgaria, Denmark, France, Greece, the Netherlands, Poland and Romania) inform defendants about their criminal procedural rights in various ways, depending on whether they are deprived or not deprived of liberty.[133] In the latter case, **generally, defendants receive the information before their first official questioning. However, the information given differs in its scope and content, and in how it is conveyed. This ranges from LEAs providing defendants with comprehensive information, both in writing and orally, to authorities handing defendants a written leaflet about rights without further explanation**.[134]

FRA calls upon Member States to put in place safeguards to ensure that individuals can effectively exercise their right to be informed about their criminal procedural rights as soon as they are suspected of having committed an offence. Member States should provide, *inter alia*, further guidance to LEAs on how to verify defendants' understanding of the information they receive about their rights. It recommends that Member States consider making it obligatory for LEAs to provide information to defendants about their rights in both written and oral formats, using non-technical and accessible language, regardless of whether such defendants are deprived of their liberty.[135]

4.4. THE RIGHT TO ACCESS LEGAL ASSISTANCE

The ECHR, in Article 6(3)(c), and the Charter, in Article 48(2), both guarantee the right to access a lawyer. The ECHR specifies that **individuals charged with a criminal offence have the right to defend themselves either personally or through legal assistance of their choosing. If a person lacks the means to afford legal assistance, the ECHR mandates that it be provided for free when justice demands**. Similarly, the Charter emphasises the guaranteed respect for the rights of defence for anyone facing criminal charges. Directive 2013/48/EU on the right of access to a lawyer provides further details on the right to access a lawyer, treating it as an **integral component of the defence rights outlined in both the ECHR and the Charter**.

132 Rights in practice: right to access to a lawyer and procedural rights in criminal and European arrest warrant proceedings, supra, p. 12.

133 Ibid. FRA selected these countries to cover different regions and legal traditions.

134 Ibid.

135 Ibid. Authorities should pay attention to situations in which defendants may be disadvantaged through a language barrier, a lack of education or a physical or intellectual disability or by being in a state of intoxication.

According to the requirements set out in the directive and the standards from the ECtHR's case law, suspects or accused persons should have access to a lawyer without undue delay and the confidentiality of their communication should be respected.[136] They shall have access to a lawyer:

a. before they are questioned by the police or by another law enforcement agency or judicial authority;
b. when investigating authorities are carrying out an investigative or other evidence-gathering act where those acts are provided for under national law (as a minimum, suspects or accused persons shall have the right for their lawyer to attend the identity parades, confrontations and reconstructions of the scene of a crime);
c. without undue delay after deprivation of liberty; and
d. where they have been summoned to appear before a court having jurisdiction in criminal matters, in due time before they appear before that court.[137]

The right of access to a lawyer plays a significant role in facilitating other defence and fair trial rights. These include the right to competent and effective legal advice and the right to have adequate facilities for the preparation of a defence, as well as procedural rights, such as the right to remain silent and the right of an accused person to not self-incriminate.[138] **Recognising it as '*one of the fundamental features of a fair trial*,'[139] the ECtHR has consistently emphasised that the right to access a lawyer serves as a crucial procedural safeguard for the right of an accused person to not self-incriminate**.[140] Furthermore, by drawing upon the recommendations of the European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT), the **ECtHR also highlighted the importance of the right of access to a lawyer as a fundamental safeguard against ill-treatment**.[141]

According to the ECHR standards, a **person should have access to legal assistance from the moment when there is a criminal charge against them**, namely when the domestic authorities have plausible reasons for suspecting that person's involvement in a criminal offence.[142] Similarly, the FRA highlights the crucial importance of defendants having access to legal assistance from the very beginning of criminal proceedings. Defendants deprived of liberty, in particular, face difficulties in accessing lawyers directly and/or in private.[143] A very important aspect also covered by the directive is **when persons, such as witnesses, become suspects or are accused during questioning by the police or other law enforcement authorities. In such situations, the police should immediately suspend the questioning and can proceed only if the person learns that they are now considered a suspect or an accused person and can exercise their rights fully**.[144]

While the right to access to a lawyer is not an absolute right, exceptionally it may be restricted. In line with Directive 2013/48/EU, **in exceptional circumstances and only at the pre-trial stage, Member States may temporarily derogate from the application of the right to access to a lawyer (a) where there is an urgent need to avert serious adverse consequences for the life, liberty or physical integrity of a person, or (b) where immediate action by the investigating authorities is imperative to prevent substantial jeopardy to criminal proceedings**.[145] According to the ECtHR, it is possible to temporarily restrict the right of access to a lawyer in exceptional circumstances, considering the particular circumstances of the

136 Directive 2013/48/EU, Article 3. See also ECtHR, *S v. Switzerland*, a. Nos 12629/87 and 13965/88, judgement of 28 November 1991 and *Marcello Viola v. Italy*, a. No 45106/04, judgement of 5 October 2006.

137 Directive 2013/48/EU, Article 3.

138 Rights in practice: right to access to a lawyer and procedural rights in criminal and European arrest warrant proceedings, supra, p. 38.

139 Ibid., p. 39. See ECtHR, *Simeonovi v. Bulgaria*, a. No 21980/04, judgement of 12 May 2017, para. 112; *Dvorski v. Croatia,* a. No 25703/11, judgement of 20 October 2015, para. 76; *Dayanan v. Turkey*, a. No 7377/03, judgement of 13 October 2009; *Ibrahim and Others v. the United Kingdom*, a. Nos 50541/08, 50571/08, 50573/08 and 40351/09, judgement of 13 September 2016, para. 255; *Beuze v. Belgium*, a. No 71409/10, judgement of 9 November 2018, para. 123; and *Salduz v. Turkey*, supra, para. 51.

140 Rights in practice: right to access to a lawyer and procedural rights in criminal and European arrest warrant proceedings, supra, p. 39. See also *Salduz v. Turkey*, supra, para. 54 and *Jalloh v. Germany,* supra, para. 100.

141 Rights in practice: right to access to a lawyer and procedural rights in criminal and European arrest warrant proceedings, supra, ibid.

142 Ibid.

143 For example, police officers or defendants' relatives call lawyers on their behalf. Sometimes, these calls are significantly delayed after the moment of arrest or detention. When such 'indirect' or delayed contact occurs, defendants cannot obtain advice at an early stage, such as to remain silent. FRA also reports that defendants deprived of liberty do not always have the possibility of talking to their lawyers in private before the first questioning and that sometimes lawyers cannot ask questions that may help them to prepare an effective defence. Where conversations happen at all, they are often short and/or take place in public corridors in the presence of police officers. See ibid., p. 37.

144 Ibid., p, 38.

145 Directive 2013/48/EU, Articles 3(4) and (5).

case (such compelling circumstances include 'an urgent need to avert serious adverse consequences for life, liberty or physical integrity in a given case'.[146]

The **ECtHR established the principles to consider when a restriction on the right of access to a lawyer is compatible with the right to a fair trial**. If there were compelling reasons for restricting the right for a defendant to have access to a lawyer, **the ECtHR considers whether such a restriction irretrievably prejudiced the overall fairness of the criminal proceedings**. The Court determined factors for assessing the impact of procedural failure at the pre-trial stage on overall fairness, including the vulnerability of the applicant and the possibility of challenging the authenticity or the quality of the evidence.[147]

CHECKLIST OF KEY POINTS ON THE PRESUMPTION OF INNOCENCE AND FAIR TRIAL RIGHTS

- ☐ Despite its paradoxical nature, the presumption of the defendant's innocence remains the cornerstone of civilised criminal procedure and criminal justice in contemporary times.
- ☐ The presumption of innocence is a fundamental right and key principle at the heart of fair trial rights protection under the ECHR, the European Charter, under the provisions of the International Covenant on Civil and Political Rights, the Universal Declaration of Human Rights, and several other international treaties and covenants, as well as under the constitutions of the EU Member States.
- ☐ The presumption of innocence concerns the following rights and safeguards: prohibition of the use of compulsion, the right to remain silent, the right to not incriminate oneself, reversal of the burden of proof and the principle that any reasonable doubts on the guilt should benefit the accused, and the right to an impartial and independent tribunal.
- ☐ Additionally, two additional fair trial rights are also inextricably linked to the effective implementation of the presumption of innocence in pre-trial investigations: the right to information in criminal proceedings and the right to access to legal assistance and to have adequate time and facilities for the preparation of the defence.
- ☐ According to Directive (EU) 2016/343, the presumption of innocence and the privilege against self-incrimination impose an obligation to ensure that the burden of proof for establishing the guilt of suspects and accused persons is on the prosecution and that any doubt as to the question of guilt is to benefit the suspect or accused person, including where the court assesses whether the person concerned should be acquitted.
- ☐ The exercise by suspects and accused persons of the right to remain silent or of the right to not incriminate oneself shall not be used against them and shall not be evidence that they have committed the criminal offence concerned.

146 Rights in practice: right to access to a lawyer and procedural rights in criminal and European arrest warrant proceedings, supra, p. 39. See also *Simeonovi v. Bulgaria*, supra, para. 117; *Ibrahim and Others v. the United Kingdom*, supra, paras. 259 and 263–265; and *Salduz v. Turkey*, supra, paras. 55.

147 Rights in practice: right to access to a lawyer and procedural rights in criminal and European arrest warrant proceedings, supra, ibid. See also *Ibrahim and Others v. the United Kingdom*, supra, paras. 263–265 and *Simeonovi v. Bulgaria*, supra, para. 118.

- ☐ While the privilege against self-incrimination presupposes that in a criminal case the prosecution and LEAs are prohibited to obtain evidence by coercive methods, the ECtHR distinguishes between testimonial and non-testimonial evidence, maintaining that the privilege and the right to remain silent do not protect against the use of coercion in obtaining material that is in the defendant's domain independently of their will (e.g. documents, blood, urine and DNA samples, etc.)
- ☐ Pursuant to Directive (EU) 2016/343, Member States may allow their judicial authorities to consider, when sentencing, cooperative behaviour of suspects and accused persons.
- ☐ Suspects or accused persons have the right to be informed about the accusation, the reasons for detention if deprived of liberty, the right to access a lawyer, the right to interpretation and translation, and the right to remain silent and to not incriminate themselves.
- ☐ Suspects or accused persons should have access to a lawyer from the moment when the domestic authorities have plausible reasons for suspecting that person's involvement in a criminal offence (the crucial importance of defendants having access to legal assistance from the very beginning of criminal proceedings is also highlighted by the FRA) and the confidentiality of their communication should be respected.
- ☐ In exceptional circumstances and only at the pre-trial stage, the application of the right to access to a lawyer may be temporarily derogated.
- ☐ In the digital age, legal systems face new challenges in preserving fair trial rights, related to, *inter alia*, the cross-border nature of contemporary crime and the use of technology in criminal proceedings.

5. ELECTRONIC EVIDENCE

Electronic evidence can be defined as any evidential information stored or transmitted in electronic form. It encompasses any data that can be used as evidence, irrespective of whether it is stored on or produced, processed, or transmitted by an electronic device. The scope of electronic evidence spans both 'content data,' such as e-mails, text messages, and photographs, and 'non-content data,' which encompasses subscriber and traffic data (e.g. routing or timing information of a message). Such data can be held by individuals in their electronic devices, legal persons such as enterprises, companies, and all sorts of institutions in their electronic devices and internal information/communication systems and a variety of providers of electronic communications and internet services. Spanning both stages of the criminal process, the pre-trial investigation and the trial stage, the electronic evidence life cycle encompasses the collection, preservation, and analysis of electronic evidence by LEAs, application (including the assessment of lawfulness and admissibility) of electronic evidence by courts, and the transfer and exchange of electronic evidence.

The impact of digitalisation in a 'new digital reality' can be observed in all segments of society, including in the fields of criminal law and criminal justice.[148] **The introduction and the extensive use of information technology has generated new forms of crimes and new ways of perpetrating them, as well as new types of evidence, including evidence in electronic form**. Using social media, webmail, messaging services and 'apps' to communicate and work has become omnipresent. Accordingly, these services and apps are often the only place where investigators can find leads to determine who committed a crime and obtain evidence that can be used in court.[149]

According to the European Commission, **electronic evidence is relevant in approximately 85 % of all criminal investigations**.[150] Bearing this in mind, obtaining evidence in a criminal case may require access to data that is stored outside a given country and/or by service providers in other Member States or third countries. As documented by the Commission, more than half of all investigations include a cross-border request to access electronic evidence. To be more specific, **in almost two thirds (65%) of the investigations where e-evidence is relevant, a request to service providers across borders (based in another jurisdiction) is needed**. The number of such requests has increased by 70% in the last 4 years.[151]

As technology progresses, **the importance of electronic evidence in criminal proceedings will continue to grow**. While all types of evidence must adhere to criminal procedural laws and handling protocols, electronic evidence has a wider scope, can be more personally sensitive, is volatile, and requires different training and tools compared to physical evidence. It demands additional and specific handling methods to preserve its authenticity, integrity, and probative value. **Effectively managing the challenges associated with acquiring, preserving, analysing, ensuring admissibility, and facilitating both internal and cross-border exchange of electronic**

148 See the Communication on Digitalisation of Justice in the European Union – A toolbox of opportunities, European Commission, Brussels, 2 December 2020, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX-%3A52020DC0710.

149 Impact Assessment – Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, European Commission, Commission Staff Working Document, European Commission, 17 April 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A1%3AFIN.

150 Ibid.

151 Ibid.

evidence necessitates a comprehensive understanding of both technological and legal aspects. This is particularly crucial in relation to upholding the presumption of innocence, ensuring a fair trial, protecting the right to privacy, and upholding other rights and safeguards for individuals who are suspected or accused of criminal behaviour.

This Section aims at a brief but comprehensive insight in electronic evidence in criminal proceedings. It provides a basis for elaborating in Section 6.1 of this Toolkit a procedural framework for handling electronic evidence in all stages of their life cycle and enhancing the practical application of the presumption of innocence by criminal justice actors.

5.1. THE DEFINITION, ORIGINS AND TYPES OF ELECTRONIC EVIDENCE

Defining the term 'Electronic Evidence' proves to be a complex task. **Various domestic and international legislators have addressed electronic evidence in diverse contexts within criminal proceedings, yet a clear definition remains elusive**. Introduced earlier in this Toolkit, the EVIDENCE project, for example, emphasises the importance of establishing harmonised procedures for handling and exchanging electronic evidence within a common European framework. The project proposed the following definition of electronic (and digital) evidence:[152]

> Electronic Evidence refers to any data[153] resulting from the output of an analogue device and/or a digital device with potential probative value, generated by, processed by, stored on, or transmitted by any electronic device. Digital evidence is a subset of Electronic Evidence that is either generated in or converted to a numerical format.

Similarly, **the European Parliamentary Research Service defines Electronic Evidence as any data that can serve as evidence, regardless of whether it is stored on or generated, processed or transmitted by an electronic device or information/communication system, such as computers, smartphones, tablets, smartwatches, household appliances, portable media (e.g. USB sticks, external hard drives), clouds, online information systems, vehicle information systems, etc**. It includes both 'content data', such as e-mails, text messages and photographs, and 'non-content data', such as subscriber and traffic data (e.g. the routing or timing of a message). **Electronic data can be held by individuals in their electronic devices, legal persons such as enterprises, companies, and all sorts of institutions in their electronic devices and internal information/communication systems and a variety of providers of electronic communications and internet services**.[154] Essentially, Electronic Evidence can be defined as any item, data or information that is stored or transmitted in an electronic format and considered admissible in court.

Electronic evidence originates from various sources. The first type of origin is physical (non-electronic) items or evidence, such as a murder weapon or the

152 See M. A. Biasiotti: A proposed electronic evidence exchange across the European Union, Digital Evidence and Electronic Signature Law Review,14(2017), p. 1, https://journals.sas.ac.uk/deeslr/article/view/2337/2289.

153 In this definition, the term data includes digital and analogical items as the latter may be transformed into digital form. See Biasiotti, op. cit., p. 4.

154 See Electronic evidence in criminal matters, European Parliamentary Research Service, September 2023, p. 2., https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI(2021)690522_EN.pdf.

bloodstain of the victim, which can be digitised—for instance, by capturing a digital photograph of the murder weapon. The second type of origin involves analogical evidence, formed in an analogue form (e.g. videotape or vinyl), which can undergo digitisation through a process to acquire a digital status. The third type of origin is digital evidence, originally in digital form as created by any digital device (e.g. computer or computer-like device). The EVIDENCE project classifies these evidence as 'electronic evidence,' recognising that, at the end of the process, they can be labelled as electronic regardless of their initial origin. Thus, **in a broad sense, electronic evidence can be understood as any probative information stored or transmitted in electronic form**. This term encompasses all types of evidence, independent of their origin or the method by which they were created, leading to a comprehensive understanding of electronic evidence.[155]

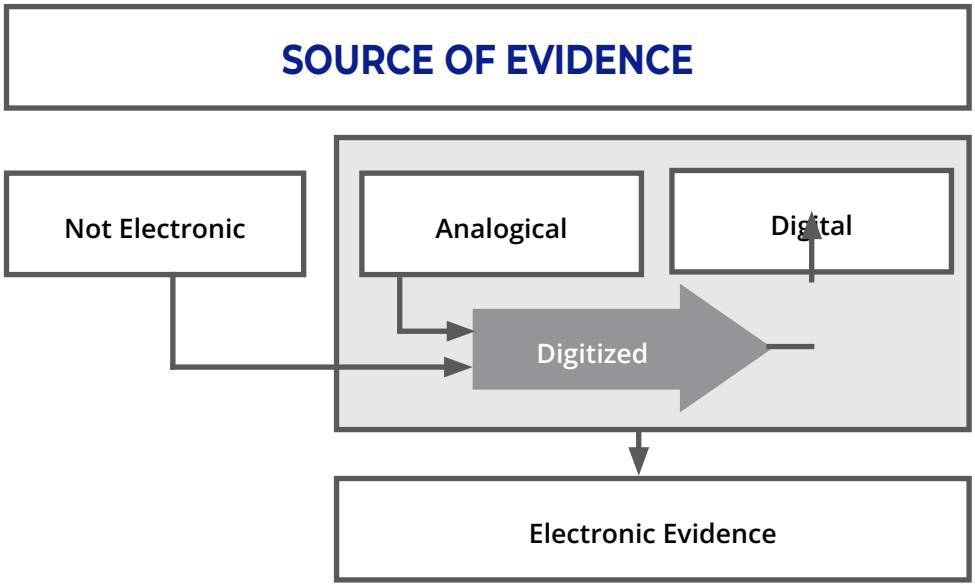

Figure 6: Source of electronic evidence

Source: M. A. Biasiotti: A proposed electronic evidence exchange across the European Union, Digital Evidence and Electronic Signature Law Review, 14(2017), p. 4, https://journals.sas.ac.uk/deeslr/article/view/2337/228

Electronic evidence can be broadly classified into two categories:

a. **Evidence from stored data**, obtained from devices storing digital information; and
b. **Evidence from data intercepted during transmission**, involving the interception of data transmission and communications.

In terms of electronic evidence types, digital forensics differentiates among logs, video footage, images, archive data, temporary files, replicant data, residual data, metadata, and data stored inside a device's RAM, if the data is considered relevant for a digital investigation and could be used in court.

155 Biasiotti, op. cit., p. 4.

These types can be further divided into (i) volatile electronic evidence and (ii) non-volatile electronic evidence. **Volatile electronic evidence** is only present while the computer is running and must be collected using live forensic methods. This includes evidence in the system's RAM (Random Access Memory), such as a program or file that is only present in the computer's memory. For instance, various types of malware, like Trojan horse programs, viruses, and worms, are designed to exist in the computer's memory only during operation, disappearing when the computer is turned off, often leaving no traces. Additionally, other volatile evidence, such as certain temporary files, log files, cached files, and passwords, is accessible to investigators only while the computer is running. RAM is cleared when the computer is turned off, leading to the loss of any present data.[156] **Non-volatile electronic evidence**, on the other hand, is evidence that persists when the electronic device lacks a power supply. Examples include files stored on hard disks, thumb drives, memory cards, etc.[157]

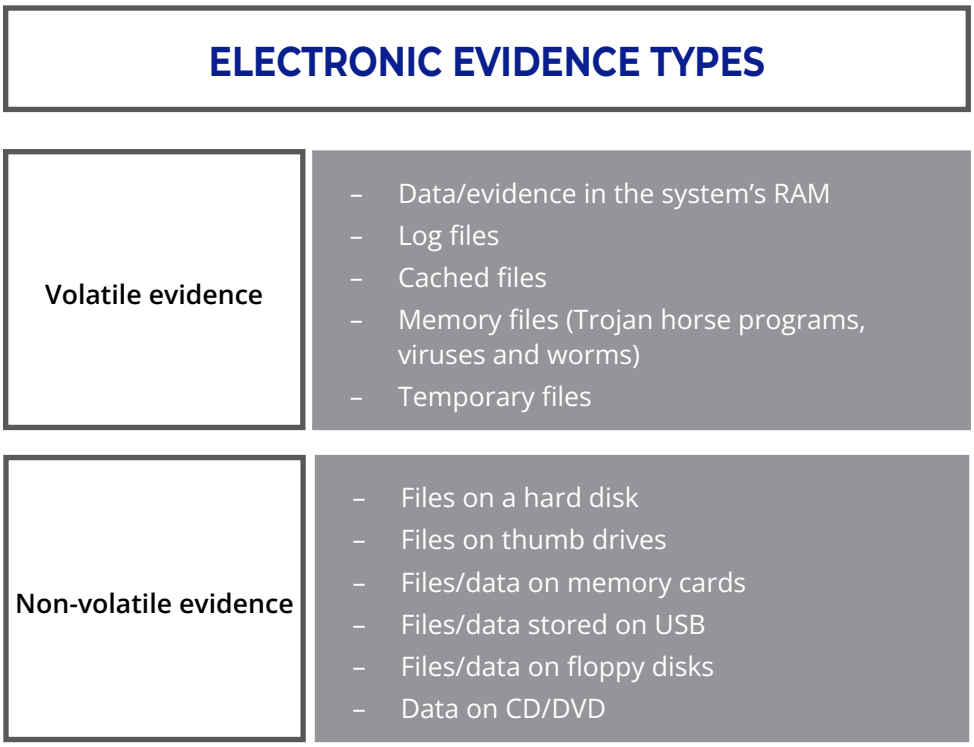

Figure 7: Electronic evidence types

5.2. THE LIFE CYCLE OF ELECTRONIC EVIDENCE

The electronic evidence life cycle encompasses the collection, preservation and analysis of electronic evidence by LEAs, application of electronic evidence by courts (including the assessment of lawfulness and admissibility), and the transfer and exchange of electronic evidence. These phases span both stages of the criminal process, the pre-trial investigation, and the trial stage. **In each phase, the presumption of innocence,**

156 L. E. Daniel, I. E. Daniel: The Foundations of Digital Forensics: Best Practices. In: L. E. Daniel and I. E. Daniel, Digital Forensics for Legal Practitioners: Understanding Digital Evidence From The Warrant To The Courtroom, Elsevier, 2012. https://www.sciencedirect.com/science/article/abs/pii/B9781597496438000043.

157 See R. A. Ramadhan, P. R. Setiawan, D. Hariyadi: Digital Forensic Investigation for Non-volatile Memory Architecture by Hybrid Evaluation Based on ISO/ESC 27307:2012 and NIST SP800-86 Framework, IT Journal Research and Development (ITJRD), Vol. 6, No 2, March 2022, p. 163, http://journal.uir.ac.id/index.php/ITJRD.

along with several other rights and safeguards for the suspected and accused individuals, assumes a significant yet distinct role. Here, the phases in the life cycle of electronic evidence are outlined briefly. A more detailed exploration, considering the roles of different actors and emphasising the preservation of the presumption of innocence and other rights and safeguards, will be provided in Section 6.1.

The **collection** of electronic evidence involves the comprehensive process of gathering items with potential electronic evidence, encompassing activities such as search, seizure, interception, and other forms of evidence gathering by LEAs. This phase includes tasks such as searching the crime scene, identifying and collecting evidence (which involves determining the items most likely to serve investigative purposes and acquiring them, issuing orders to produce data to service providers, etc.), implementing anti-contamination precautions (including prioritising time-sensitive potential evidence and addressing risks of loss or corruption, issuing requests for data preservation to service providers, etc.), and appropriately packaging and labelling electronic evidence. Documentation is crucial at every step to create reports detailing the activities undertaken during the collection process.

During the collection of electronic evidence, LEAs may encounter challenges arising from encrypted or password-protected electronic devices and information systems. A pivotal question arises concerning whether a suspect is obligated and can be compelled to divulge data to LEAs, including passwords, PINs, and other access keys for computers, e-mails, and applications. There is no clear or uniform answer to this question: considering the presumption of innocence (ensuring the right to remain silent and not incriminate oneself), suspects and defendants are generally not obliged to provide evidence incriminating them, including data within electronic devices, and are not required to share data, including passwords, PINs, and decryption/private keys, with LEAs. Nevertheless, in practice, some Member States have incorporated specific legal provisions in their laws, mandating suspects to hand over passwords or data in an unencrypted format, with potential consequences if they refuse to comply. In certain Member States, LEAs may attempt to incentivise cooperation through promises or threats, suggesting that collaboration could lead to expedited proceedings or lenient treatment.[158] The intricate legal issues, particularly those related to human rights, will be explored in greater detail in Section 6.1 of this Toolkit.

Upon collection, electronic evidence must undergo **preservation** before LEAs can analyse it and present it at trial. Preservation involves the crucial process of maintaining and safeguarding the integrity and original condition of potential electronic evidence. This encompasses the creation of a secure safety copy and its storage to prevent any alterations. While ensuring the preservation of evidence is vital throughout every phase of handling electronic evidence, access to the evidence must be restricted solely to authorised personnel. Throughout the electronic evidence life cycle, copies of the evidence will be required for dissemination to various competent authorities, including LEAs, digital evidence professionals, courts, and others. This ensures that relevant parties have access to the evidence as needed.[159]

Subsequently, the gathered electronic evidence is subjected to **analysis** by forensic examiner(s), culminating in the production of a final document or report by LEAs for presentation in court. This phase involves both technical and legal considerations. If investigators did not acquire a password, PIN, encryption key, etc., during the collection phase decryption becomes LEAs' task at this

158 INNOCENT Report, supra, pp. 31–33. See also the Presumption of innocence and related rights - Professional perspectives. Report, European Union Agency for Fundamental Rights, 2021, https://fra.europa.eu/en/publication/2021/presumption-of-innocence.

159 Biasiotti, op. cit., pp. 4–5.

160 Ibid., pp. 6–7.

stage, presenting technical challenges. Another vital aspect in this phase is establishing the 'chain of custody.' This entails maintaining a documented record of the evidence's handling and storage to ensure its integrity and admissibility. Legal concerns at this juncture involve, *inter alia*, identifying criteria for evidence to be presented at trial, upholding the right to an effective defence, and recognising potential legal privileges. The final step in this phase of the e-evidence life cycle is the presentation of results in a comprehensive report. This report should encapsulate factual findings, interpretations, and expert opinions. The court relies on this report to scrutinise all relevant findings, technical and non-technical explanations, and the nuances of the case.[160]

During the trial phase, LEAs must present a final document or report before the court. The court is tasked with evaluating the authenticity, legality, and **admissibility** of electronic evidence. Furthermore, the probative value of the evidence is assessed, and it is used if its credibility is established. Judges, playing a central role in this stage of the process, are required to comprehend the technical intricacies of electronic evidence, particularly its origin and acquisition. They must also grasp the relevant technology and understand how it was employed in obtaining the electronic evidence presented to them. Without this understanding, making informed and sound decisions regarding the admissibility of the evidence becomes a challenging task. In view of the above, in this phase, in addition to judges, court experts and expert witnesses also play an important role.[161]

The **transfer and exchange** of electronic evidence can occur in various phases in the electronic evidence life cycle, and it is crucial to distinguish between sharing within a country and across borders—making a clear differentiation between transfer and exchange. While a transfer may transpire between different agencies within the same country, an exchange typically involves competent national authorities from different countries engaging in cross-border collaboration within the field of cooperation in criminal matters. As criminal investigations, both domestic and cross-border, increasingly depend on data and evidence held by various service providers, the transfer and/or exchange of electronic data and evidence among domestic participants in the criminal judicial process and across jurisdictions poses a significant challenge to law enforcement and judicial authorities, frequently facing difficulties in accessing this data and evidence. Recognising the gravity of these challenges, the EU has taken substantial steps to enhance international cooperation in the criminal sector with improving existing mechanisms that facilitate the exchange of electronic evidence within the EU legal framework.[162]

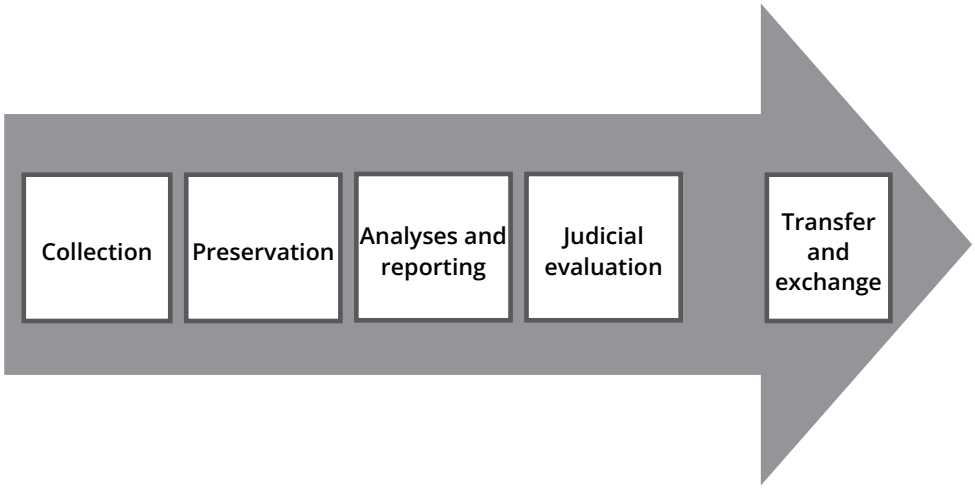

Figure 8: Electronic evidence life cycle

161 FORMOBILE Guidance to Checklist Preparation for Legal Practitioners, supra, p. 42.

162 Ibid., pp. 45–46. See also Sections 3.2.2 and 6 of this Toolkit.

5.3. HANDLING AND ADMISSIBILITY OF ELECTRONIC EVIDENCE: TOWARDS A COMMON LEGAL FRAMEWORK AND STANDARDISED PROCEDURES

The EVIDENCE project's overview of the legislation and practices currently in place in the European Union and its Member States revealed that, **when it comes to the collection, preservation and analyses of electronic evidence by LEAs, judicial assessment of admissibility, and sharing of electronic evidence, there were significant differences among legal frameworks and practices of Member States** and that **there was clearly no comprehensive international or supranational legal framework** relating to it.[163] While it is true that some countries have adapted their legislation to accommodate electronic evidence, others rely on general criminal procedure provisions and apply them to electronic evidence. Evidence rules vary considerably even among countries with similar legal traditions. **In certain countries, traditional investigative powers might be general enough to apply to electronic evidence, while in other countries traditional procedural laws might not cover specific issues regarding electronic evidence**, making it necessary to have additional legislation. The review pointed to the fact that **significant differences in national legislation and approaches make the handling of electronic evidence difficult across jurisdictions**.[164] Notable disparities in internal criminal procedural law pertaining to electronic evidence in the project partner's countries were also identified by the review carried out within the INNOCENT project.

There is a need for the establishment of a common legal framework and standardised procedures, which should address the entire life cycle of electronic evidence, embracing both (a) the Regulation of the collection, preservation, use, and transfer and exchange of electronic evidence, and (b) the guidance of policy makers, LEAs, and judicial authorities in considering and handling electronic evidence. Such a unified legal framework should encompass common and specific rules, definitions, standards, and procedures for collection; guidelines for preservation and use; specific investigative measures; admissibility based on mutual trust; transfer of electronic evidence; provisions regulating the role of private sector participants; Joint Investigation Teams; and effective cross-border regulation.[165]

Nevertheless, there are various international and European legal instruments and policy documents currently in place that hold relevance in this context. Notably, the EU and CoE legal mechanisms facilitating cross-border judicial cooperation in criminal matters, as discussed in Section 3 on international and EU legal framework, encompass tools such as the EU and CoE Mutual Legal Assistance (MLA) mechanisms and European Investigation Order (EIO) procedures, as well as European Production and Preservation Orders, which are to be transposed into national law by EU Member States by 18 February 2026. Sections 6.2 and 6.3 of this Toolkit will delve into some of these mechanisms.

163 Biasiotti, op. cit., p. 6. See also Overview of existing legal framework in EU Member States, European Informatics Data Exchange Framework for Courts and Evidence (EVIDENCE), D3.1, http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d3-1-411.pdf. The EVIDENCE project conducted a survey in 13 Member States in such a way that a fair representation of 'families of law' and of different regions of Europe (i.e. common law/ civil law; Nordic countries/ Southern countries/Eastern Europe/ Central Europe, etc.) was ensured.

164 Biasiotti, op. cit., p. 6.

165 Ibid., pp. 6–7.

CHECKLIST OF KEY POINTS ON ELECTRONIC EVIDENCE

- ☐ Approximately 85% of criminal investigations find electronic evidence to be pertinent. In nearly two-thirds (65%) of cases where electronic evidence is relevant, seeking assistance from service providers across international borders is required. The number of such requests has increased by 70% in the last 4 years.
- ☐ Broadly speaking, Electronic Evidence can be defined as any evidential information stored or transmitted in electronic form. This definition encompasses all varieties of evidence, regardless of their source or the method by which they were generated. Electronic evidence has a wider scope, can be more personally sensitive, is mobile, and requires different training and tools compared to physical evidence.
- ☐ Electronic evidence encompasses any data that can be used as evidence, irrespective of whether it is stored on or produced, processed, or transmitted by an electronic device. This includes devices like computers, smartphones, tablets, smartwatches, household appliances, portable media (e.g. USB sticks, external hard drives), cloud storage, online information systems, and vehicle information systems, among others. The scope of electronic evidence spans both 'content data,' such as e-mails, text messages, and photographs, and 'non-content data,' which encompasses subscriber and traffic data (e.g. routing or timing information of a message). Such data can be held by individuals on their electronic devices, legal persons such as enterprises, companies and all sorts of institutions in their electronic devices and internal information/communication systems and a variety of providers of electronic communications and internet services.
- ☐ The electronic evidence life cycle encompasses the collection, preservation, analysis, use (including the assessment of lawfulness and admissibility), and the transfer and exchange of electronic evidence.
- ☐ Currently, the EU and CoE legal mechanisms pertaining to electronic evidence encompass tools facilitating cross-border judicial cooperation in criminal matters (such as MLA mechanisms, EIO procedures, and European Production and Preservation Orders). However, there is a lack of a comprehensive and unified international or European legal framework addressing the entire life cycle of electronic evidence.

6. PROCEDURAL FRAMEWORK FOR HANDLING AND ADMISSIBILITY OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS – ENHANCING THE PRESUMPTION OF INNOCENCE AND FAIR TRIAL RIGHTS FOR SUSPECTS AND ACCUSED PERSONS

The process of acquiring and handling electronic evidence undergoes distinct phases within the life cycle of e-evidence, occurring during both the pre-trial and trial stages of criminal proceedings. While various models exist for conceptualising the life cycle of electronic evidence, this Toolkit, though not exclusively, aligns with the 9-step conceptual framework of 'e-evidence governance' presented by the FORMOBILE project in their Checklist Guidance Document.[166] The phases outlined in this document's e-evidence governance framework are as follows:

1. Pre-acquisition,
2. Acquisition,
3. Preparation,
4. Analysis,
5. Reporting,
6. Judicial Evaluation,
7. Sharing,
8. Archiving, and
9. Deletion.

Although the primary focus of the Checklist Guidance Document is to provide guidance for acquiring, analysing, and using electronic data and evidence stored in mobile phones with emphasising investigative and digital forensics perspectives, its applicability extends to other perspectives (e.g. actors of the criminal justice system) and types of electronic devices. Accordingly, in this Toolkit the 'digital chain' and the phases of the electronic evidence life cycle referred to by FORMOBILE have been condensed and reorganised as follows:

- **Pre-trial Investigation Stage** (Collection, Preservation, Analysis);
- **Trial Stage** (Judicial Assessment of the Lawfulness and Admissibility, Role of Court Exerts and Expert Witnesses);
- **Cross-Border Access to and Exchange** of Electronic Evidence.

166 See the FORMOBILE Guidance to Checklist Preparation for Legal Practitioners, supra, p. 8.

In this Section of the Toolkit, the different roles (i.e. rights and obligations) that each of the main actors in criminal procedures is entitled to are analysed. We depart from the major EU and CoE legal texts and the Roadmap's instruments for strengthening the presumption of innocence and other procedural rights of suspected and accused persons in criminal proceedings, as well as cornerstone EU instruments which relate to a cross-border dimension, i.e. the European Investigation Order (EIO) and existing Mutual Legal Assistance (MLA) legal documents. The case law practice of the ECHR and the rulings of the CJEU, relevant to both stages of the criminal procedure is also taken into consideration.

As highlighted by FORMOBILE, a **crucial aspect in the successful handling and managing of electronic evidence is recognising that each step in the evidence life cycle is interconnected**. Professionals engaged in various stages of this process must perceive themselves as integral components of a holistic and interlinked system, geared towards the overarching objective of facilitating criminal justice decisions based on reliable evidence that has been forensically processed in accordance with the law. **Processing electronic evidence is not a mere sequential progression of isolated steps performed independently by forensic and legal experts. Instead, it forms an integrated entity that demands well-organised communication and even a hierarchical structure among all involved actors. This includes, but is not limited to, LEAs (investigators and forensic experts/examiners), prosecution offices (prosecutors), courts (judges), court-appointed experts, expert witnesses, and defence lawyers. Establishing effective communication and a hierarchy among these stakeholders is pivotal to ensuring a seamless and lawful progression of the electronic evidence handling process**.[167]

6.1. PRE-TRIAL INVESTIGATION STAGE: COLLECTION, PRESERVATION AND ANALYSIS

Broadly speaking, the pre-trial phase of criminal proceedings concerns the pre-trial investigation and indictment procedure. The purpose of the pre-trial investigation is to determine all significant circumstances of a crime, identify the person who might have committed that crime and create the conditions for a proper hearing of the case in court quickly and fully. Normally, the pre-trial investigation is organised and headed by a prosecutor and carried out by investigating officers. The prosecutor may decide to carry out the whole pre-trial investigation, or part of it, in person. Some parts of the investigation procedure may also be organised, headed, and carried out by a pre-trial investigating judge. **All information which confirms or disproves the circumstances of a case during the pre-trial investigation is usually called evidence, although in this stage of the criminal procedure it would be more accurate to call it material or data. It will be for the court to decide during its hearing whether the material and/or data which has been collected will become evidence**.

167 Ibid., pp. 7–8.

The prosecutor or investigating judge has (or should have) the role of issuing, coordinating, and controlling the investigation measures and leading the investigators during the different phases of the chain of evidence, until the indictment is approved by the court.[168] With regard to electronic data and evidence, the process during an investigation can be divided into several phases, which include **collection, preservation and analysis** of electronic evidence. These phases can be split into further steps (see below) which, all together, should lead to the preparation of electronic material by LEAs that serves as evidence in court. **In each of these phases, the presumption of innocence and several other rights and safeguards play a significant but distinctive role if a fair and just trial is to be ensured to the person suspected or accused of committing a criminal offence**.

6.1.1. Collection

As outlined in Section 5.2 of this Toolkit, **the collection of electronic evidence refers to the comprehensive process of gathering items or materials that encompass potential electronic evidence in its broadest sense**. This encompasses pre-collection activities, including preparation, planning, and the examination of the crime scene, as well as various methods employed by LEAs for evidence gathering. LEAs may conduct these activities autonomously, employing methods such as acquisition, seizure, interruption, etc., or in collaboration with telecommunications operators, internet providers, or other private entities.

Pre-collection activities encompass the preparatory and planning stages for the collection of electronic evidence. This involves **systematically identifying, during the examination of the crime scene, items with the potential to serve as evidence** and contribute meaningfully to the investigation. Additionally, these activities may involve **seeking a court order or another appropriate legal measure when data, potentially constituting electronic evidence, is stored by service providers**. The main legal issue during the pre-collection phase is establishing the appropriate legal basis for initiating the criminal investigation. This necessitates **a thorough understanding of the relevant legal frameworks and regulations. Equally significant is the training of investigators to proficiently operate technical equipment and adhere to legal and IT-forensic standards**.[169]

Establishing the correct legal basis for commencing a criminal investigation and implementing investigative measures is crucial. The selected legal basis delineates the procedural guidelines, determining both the legal and technical procedures, the extent of permissible actions, and their limitations. This choice clarifies the regulations that govern the collection, preservation, use, and potential exchange of electronic data, taking into account considerations such as the presumption of innocence, data protection, and other procedural rights and safeguards. **Failure to define this legal basis accurately may result in evidence being deemed inadmissible, thereby losing its inculpatory or exculpatory effect**.[170]

168 Ibid.
169 Ibid., p. 9.
170 Ibid., p. 17.

The acquisition of electronic evidence is subject to regulation under both national and international legislation, encompassing domains such as criminal law, fundamental rights, and privacy and data protection. Essential inquiries in this context revolve around determining the nature of the data and evidence to be collected, the methodologies employed for acquisition, and the boundaries set on the collection process. These questions inherently give rise to legal considerations that must be thoroughly examined during the electronic evidence collection process.

Given the absence of harmonised European rules at present, the selection of a relevant legislative basis aligns with the respective national legislation governing the seizure and search of electronic devices and the data they contain.[171] **In the context of countries involved in the INNOCENT project, our assessment reveals absence of explicit provisions within the legislation of the majority of partner countries regarding the (pre)collection, preservation, and use of electronic evidence**. **Instead, reliance on general provisions is prevalent, with these regulations being extrapolated and applied to electronic evidence.** While traditional investigative powers may, in principle, be broad enough to encompass electronic evidence, traditional procedural laws may fall short in addressing specific issues related to electronic evidence. This gap necessitates potential amendments to existing legislation to adequately cover electronic evidence-related matters. Irrespective of the approach, individual countries and their competent authorities will establish their own legal basis for investigative measures, whether through general or specialised laws.

Apart from their domestic criminal law regulations regarding investigative measures, the LEAs of the countries must also consider constitutional, international, and EU human rights provisions related to criminal proceedings and investigations. These encompass various provisions within the ECHR, the Charter, and the Roadmap Directives, in particular Directive 2012/13/EU on the right to information, Directive 2013/48/EU on the right of access to a lawyer in criminal proceedings, and Directive 2016/343/EU on the strengthening of certain aspects of the presumption of innocence. Notably, these provisions address key aspects such as the **presumption of innocence**, the **right to access a lawyer**, and other rights integral to ensuring a fair trial. Additionally, these legal frameworks include provisions concerning the **protection of privacy and personal data**, as detailed below.

The FORMOBILE project draws attention to another important aspect of the pre-collection phase of e-evidence governance by pointing out that in addition to establishing suitable legal basis for collecting and analysing electronic evidence, a secondary question of capacity to perform the task should also be considered. **Due to the volatile nature of certain types of electronic evidence, there is a risk that evidence could be lost, damaged, or deleted by untrained staff attempting to move or recover electronic evidence without suitable skills or equipment. This potential jeopardy introduces legal challenges, particularly concerning the chain of custody and the interpretation of data**. Incompetence of investigators may be asserted, or allegations of the defence losing exculpatory evidence could arise. Hence, it becomes imperative that duly authorised staff can demonstrate both suitability and competence in executing the technical tasks essential for

171 171 Ibid., p. 18.

the accurate collection of electronic evidence. **Ensuring this competence requires assigned personnel to undergo appropriate specialised training in mobile device data acquisition**.[172]

The *Collection phase* involves the acquisition of items (i.e. computers, tablets, mobile phones, USB sticks or any other electronic devices) and data contained in these items which are most likely to serve the purposes of the investigation. The investigators (i.e. the LEAs) may resort to different ways of gathering electronic data and evidence, which are either in their own capacity or need to be performed through the assistance of the telecommunications operators and internet providers or other private or public entities (if/when such data and evidence is stored in the cloud or it concerns a suspect's virtual identity or past communication via e-mail, social network apps or other means of electronic communication**). This central phase of electronic evidence life cycle implies seizure or other forms of inquisition of electronic devices and physical, logical or manual extraction of data from such devices**.

It is worth noting that the collection phase also includes **obtaining from the suspected/accused persons' (or other persons') passwords, PINs and decryption keys of their electronic devices** or *ex post* forensic decryption of those devices (see *infra*). In cases where potentially evidential electronic data is stored by a service provider, the collection process involves presenting a court order or an equivalent legal basis to compel the provider to furnish the electronic data to LEAs. The collection phase also concerns *ad hoc* use and documentation of specialised tools and techniques, including the use of a Faraday bag.[173] These measures are employed to safeguard the integrity and authenticity of data and evidence during the collection process.

Referencing Simonato, the FORMOBILE Checklist Guidance Document delineates two primary modes of data collection:

- access to stored data; and
- live observation.

When gathering stored data, the common approach involves accessing a device or a cloud location to retrieve historical records of activities. In contrast, live observation may entail monitoring on-screen content or capturing visual footage of the display, without undergoing a forensic extraction process. Consequently, the chosen method of acquisition can introduce distinct technical standards and legal considerations, particularly in relation to human rights obligations. Human rights issues are also raised when LEAs decide on which electronic data to collect and which limits apply for its acquisition. This involves **finding a balance between the State's legitimate interest in investigating and prosecuting crimes and the imperative to protect the fundamental rights and freedoms guaranteed to individuals.**[174] This intricate interplay between the interests of investigation and effective crime prosecution on one side and the preservation of fundamental rights and freedoms on the other will be addressed in Subsection 6.1.4.

172 Ibid.
173 Ibid., p. 21.
174 Ibid., p. 25.

6.1.2. Preservation

While there may arise a necessity for the on-the-spot use and documentation of particular tools and techniques—such as implementing anti-contamination measures, prioritising time-sensitive and at-risk evidence, using Faraday bags, and requesting data preservation from service providers or third parties—to guarantee the integrity and authenticity of evidence, it is important to recognise that the **formal preservation of electronic evidence constitutes a separate phase in its life cycle**. This preservation phase is pivotal in the overall process.

Preservation should be focused on the maintenance of the electronic data to guarantee that, irrespective of the time frame, the retention process is able to withstand judicial scrutiny (the principles and safeguards applicable must ensure that the evidence withstands the same scrutiny as to admissibility, authenticity, and persuasiveness). National legislation should be guiding in the process by determining which evidence is to be preserved, how and for what duration.[175]

In connection with this matter, the INNOCENT project has determined that neither international and EU law nor the domestic laws of the participating countries provide detailed regulations specifying how the preservation of gathered data in electronic form should be conducted. Consequently, it appears that this aspect of pre-trial investigation and electronic evidence handling has been entrusted to the Member States' general criminal procedure rules (or specific ones if/where they exist) and the discretion of investigators. Nevertheless, irrespective of the prevailing domestic criminal (and constitutional) laws, LEAs should adhere to international and EU human rights law related to pre-trial investigations and adhere to 'good practices' during the pre-trial stage of criminal proceedings when carrying out the preservation of electronic data/evidence.

> The preservation phase is focused on ensuring the integrity of devices and data, maintaining their forensic readiness, managing the chain of custody through documentation of each step of data handling and transformation, and preparing the collected data for analysis by a forensic examiner. Within this phase, the seized and other electronic raw data undergo processes such as decryption, conversion, cleaning, categorisation (distinguishing between relevant and irrelevant data, privileged and other data, etc.), packaging, labelling, and overall preparation for subsequent analyses.

Typically, **electronic data is safeguarded by transferring it onto another suitable data carrier, ensuring the preservation of the data's identity and integrity, and maintaining its potential for use in subsequent processes**. Alternatively, an identical copy of the entire data carrier is made, with careful attention to maintaining the integrity of the copied data. In cases where these approaches are not feasible, the seized electronic device should be securely sealed. Ideally, only the specific section of the electronic device containing the targeted data should be sealed.

Preservation, as well as subsequent analysis, must be conducted by a qualified and experienced professional. Access to the evidence should be restricted exclusively to individuals authorised to handle and process such

175 Ibid., p. 50. See also Guidelines for digital forensics first responders: Best Practices for search and seizure of electronic and digital evidence, Interpol, March 2021, and F. M. Granja, G. D. Rafael: The preservation of digital evidence and its admissibility in the court, International Journal of Electronic Security and Digital Forensics, 9(1), 1–18. 2017, pp. 5, 8.

evidence. Those within LEAs and other entities with access must ensure the continuous preservation of electronic evidence during the handling process. At any stage in the electronic evidence life cycle, there may be a need to provide copies of the evidence to various competent authorities or disclose it, at least partially, to the defence.

Prior to the seizure and/or search of an electronic device, including cases where the device has not been seized, and before the extraction of electronic data, investigators may request the owner or user to take necessary and feasible measures to prevent the destruction, modification, or concealment of data. The INNOCENT project has determined that this conduct by the holder or user of an electronic device is obligatory under the domestic criminal law of all participating countries. However, whether investigators, in accordance with domestic law, can mandate such behaviour on suspects and accused persons, and whether non-compliance can lead to punishment, represents a legal issue with no definitive answer, akin to the question related to the obligation to provide password information. This will be further explored in Subsection 6.1.4.

The authorities (i.e. investigators) should invite the holder or user of the electronic device, as well as the suspect or defendant or their legal representative, or an authorised expert, to be present during the preservation of electronic data/evidence. In the event of non-response to the invitation, the security of the data and the creation of a copy shall proceed in their absence. In the absence of specific provisions, domestic law should consider general procedural provisions related to search and seizure.[176]

When securing data in electronic form, **a written record or minutes should be made.** The control value (e.g. hash value) and the method of its calculation shall be also written into it. In any case, the minutes should provide the possibility of subsequent verification of the identity and integrity of the preserved data. A copy of the minutes should be handed over to the person who was present when the data was preserved.[177]

Regardless of whether the electrical device was seized or not, the **preservation process should be carried out in a way that interferes as little as possible with the rights of persons who are not suspects or accused persons, and in such a way as to protect the confidentiality of the data and to not cause disproportionate damage** due to the temporary inability to use the electronic device.[178]

When seizing and securing evidence in electronic form, **LEAs should, in accordance with the possibilities given the circumstances of the investigation, check whether the seized material contains protected data that the suspect entrusted to the legal representative**. Such data should be extracted, preserved, and handed over to the court for safekeeping.[179]

According to the domestic criminal laws of most participating States in the INNOCENT project, **evidentiary material is retained for the duration necessary for legal proceedings**. This principle generally extends to copies of secured evidence in electronic form. The electronic device itself is preserved until the data is stored in a manner that guarantees the identity and integrity of the secured data. Adhering to good practice, **legal regulations should also establish the maximum permissible duration for storing electronic data**. In situations where making a copy of the data is not feasible, the electronic device or the specific part containing the data is retained for the required duration of

176 See, for example, Article 219.a of the Criminal Procedure Act of Slovenia (Official Gazette of the Republic of Slovenia, No 176/21 – officially consolidated text).

177 Ibid.

178 Ibid.

179 Ibid.

legal proceedings. In such instances, it becomes especially crucial to impose a time-limited restriction on storage.[180]

Finally, **copies of electronic data that are not relevant to the investigation and for which there is no other legal reason to be retained should be removed from the criminal record and deleted**. A record should be made and sent to the competent official bodies (investigating judge and State prosecutor) and the owner or user of the seized electronic device.

6.1.3. Analysis

To be prepared for and presented in the court, electronic evidence must be analysed by forensic examiner(s) and a report of the LEAs must be produced. This phase consists of activities where data that were extracted from electronic devices are evaluated either as inculpatory or exculpatory to prove or disprove the elements of the prosecution's case. This phase includes both technical and legal aspects.

As for the *technical part*, the **forensic examiner(s) should choose and apply reliable IT-forensic tools and methods for extraction (if not already done in the earlier phases), preparation, analysis and presentation of collected electronic data**. Before analysis, the original copy must be safeguarded and any analysis must be done on a suitably protected copy of the data. **If passwords, PINs, encryption keys, etc. are not obtained from suspects or third persons when seizing electronic devices, decryption must be performed at this stage. A further challenge for investigators is that electronic devices often store a huge amount of data that needs to be analysed**.[181] While these may be a challenging task technically, in practice, LEAs can take advantage of cutting-edge IT-forensic technologies, offering password recovery tools and data extraction solutions.

Due to its overall volatile nature, handling electronic evidence presents different and more complex challenges compared to handling traditional evidence. Electronic evidence can be easily modified, removed, or contaminated by new data, etc. In addition to this, it can easily cross jurisdictions. Therefore, to ensure the authenticity, integrity, and reliability of the data, and for the evidence to be accepted at trial, **it is of paramount importance that the investigator(s) maintain the *chain of custody***. The chain of custody aims at documenting where, when, why and how certain actions were taken, and by whom (including whether that person was qualified to do so). It shows in detail how the evidence was handled at every stage of the investigative process, from evidence discovery onwards. This applies to all individuals involved in the process of acquisition, collection, preservation, analysis and any other type of handling. It should include the appropriate time records and contextual information of what was done.[182]

When analysing data, **forensic examiners should act as neutral finders of fact and should apply rigorous scientific standards to ensure that the analysis has evidentiary value**. Applying scientific method begins with

180 The Slovenian criminal procedure law, for example, provides that in such cases LEAs may keep the seized electronic device or parts of the electronic device for a period of maximum 6 months from the date of acquisition, unless the seized electronic device was used to commit a crime or the electronic device itself is evidence in criminal proceedings. See ibid.

181 Large-capacity media typically seized as evidence in a criminal investigation, such as computer hard drives and external drives, may be 1 terabyte (TB) or larger. This is equivalent to about 17,000 hours of compressed recorded audio. See M. Novak, J. Grier, D. Gozales: New approaches to digital evidence acquisition and analyses, National Institute of justice Journal, 7 October 2018. https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis.

182 See the FORMOBILE Checklist Guidance Document, supra, pp. 32–34.

gathering facts and forming a hypothesis based on the available evidence. Examiners should be cognisant of the possibility that their observations or analyses are incorrect. Therefore**, to assess the veracity of our hypothesis, they need not only to seek supporting evidence, but also to consider alternate possibilities**. The process of trying to disprove the hypothesis involves performing experiments to test underlying assumptions and gain a better understanding of the digital traces they are analysing.[183] Furthermore, when carrying out the forensic analysis, the **electronic device examiner should be able to determine facts about the data, not merely recover it. They must understand that they are not just dealing with digital data, but with potential criminal evidence** which needs to be not only presented in court as such, but to also be understood by all courtroom participants. In many proceedings, the so-called compartmentalisation is visible in the courtroom when forensic specialists try to explain their findings but are not sufficiently understood by judges. In addition to this, **it is also crucial to acknowledge any assumptions and biases, as the accurate interpretation of data often hinges on the examiner's technical judgment**. Therefore, the qualifications and expertise of the examiner emerge as paramount factors in this regard.[184]

The *legal issues* at this phase concern, *inter alia*, **data distinction, identifying the legal regime applying to the data which are to be analysed, guaranteeing the presumption of innocence, the right to effective defence and other fundamental rights of a suspect or accused person, and identifying the potential legal privilege(s).**

Referring to Stoykova, the FORMOBILE Checklist Guidance Document emphasises **the importance of distinguishing between various types of electronic data** during analyses conducted by forensic examiners. Specifically, the analysis should differentiate between data constituting evidence, confidential data possibly subject to legal privilege, and irrelevant data.[185] A significant consideration when analysing electronic data is **identifying which data or portion thereof is subject to legal privilege.** This involves determining what data is protected under the right to remain silent or constitutes privileged information between a lawyer and a defendant. Properly labelling the data is essential to enable the defence to distinguish where confidential information begins and ends. Furthermore, **clear establishment of data ownership is imperative**, particularly in cases where an electronic device has multiple users or when data stored on a cloud is subject of the analysis. The legal framework governing the data depends on the identity of the data owner/originator. In principle, national legislation should define the legal regime, establishing distinct rights, protections, and proportionality tests based on whether the data owner is the defendant, witness, victim, third party, etc.[186]

In addition to the above considerations, **forensic investigators are required to thoroughly document their analysis, including the reasoning applied and any assumptions made**. According to the so-called *Law Enforcement Directive*,[187] it is crucial to establish a clear distinction between data grounded in information and data derived from personal assessments. **Forensic investigators must demonstrate adherence to the standard operating procedures of LEAs. Like the preservation phase, the defence should be afforded the right to consult, comprehend, and potentially conduct alternative analyses during this stage of criminal proceedings**. This allowance is particularly important as national law might restrict these activities at later stages if the defence has not declared its intention to do so at the initial stage.[188]

183 Ibid. See also E. Casey: Introduction, in E. Casey (ed.): Handbook of Digital Forensics and Investigation, Elsevier 2010. For instance, when examining metadata embedded in a specific file type, it is important to perform tests involving that file type to explore the relationships between common actions and associated application metadata. When forensic examiners are provided with an alternative explanation offered by the defendant, they have a duty to test such defence claims thoroughly. However, there is no ethical requirement that forensic examiners fully investigate any or all potential defences; to do so is generally impractical.

184 FORMOBILE Guidance to Checklist Preparation for Legal Practitioners., supra, p. 33. See also Stoykova, op. cit., pp. 2, 8–10.

185 FORMOBILE Guidance to Checklist Preparation for Legal Practitioners, supra, ibid. See also Stoykova, op. cit., p. 13.

186 FORMOBILE Guidance to Checklist Preparation for Legal Practitioners, p. 34.

187 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, OJ L 119, 4.5.2016, p. 89–131. Pursuant to Article 7 of the Directive, Member States shall provide for personal date based on facts to be distinguished, as far as possible, from personal data based on personal assessments.

188 FORMOBILE Guidance to Checklist Preparation for Legal Practitioners, p. 34. It is worth noting here that during the round table discussions which were carried out at the national capacity events in the framework of the INNOCENT project, certain participants pointed out that the opposite is true in their jurisdictions, namely, that the right to comprehend the date is only afforded during the trial stage of the criminal proceedings.

During the analysis phase, as well as in any other stage of the electronic evidence life cycle**, investigators are obligated to adhere to the procedures and standards to prevent violations of the presumption of innocence, the right to access a lawyer, the right to a fair trial, privacy rights, and other legal protections**. Matters pertaining to reinforcing the presumption of innocence and ensuring respect for fair trial rights and legal safeguards will be discussed in Subsection 6.1.4.

Upon completing their analysis, forensic examiners must generate a comprehensive final report. **The presentation of results in the report should encompass factual findings, interpretation, and expert opinions**. This report and presentation constitute critical steps in the electronic evidence life cycle, as the court will scrutinise the report for all relevant findings, along with technical and non-technical explanations of the case and its issues. To establish the credibility and authenticity of the evidence, investigating officers must affirm the forensic training they have undergone, the investigative skills employed, the process used for preserving electronic evidence, and the tools used for acquiring and analysing the evidence, all in preparation for presentation in court.[189]

6.1.4. Electronic evidence in the pre-trial investigation: Strengthening the presumption of innocence and a fair trial

This Subsection of the Toolkit explores the implications of the presumption of innocence (and fair trial rights) when electronic data/ evidence are gathered, preserved, and analysed by LEAs in pre-trial investigation. It explores the challenges posed by gathering of electronic evidence in criminal investigations regarding the human rights and procedural safeguards. Additionally, the Subsection examines how technology-assisted investigations affect criminal procedure and identifies key issues that could compromise the presumption of innocence and impartiality in investigations. The findings highlight the need for enhancement of fundamental rights standards and implementation of validation procedures when dealing with electronic evidence to ensure a fair trial to the suspects and accused persons and to protect all parties involved in criminal proceedings.

Building on insights from Stoykova, the FORMOBILE project has highlighted a range of issues and challenges in technology-assisted pre-trial criminal investigations. **The early use of technology often compromises the principle of the presumption of innocence**. Problems arise from shortcomings in digital forensic practices, inappropriate and inconsistent technology use, outdated procedural guarantees, and issues within the digital forensic practice. Examples include **ineffective pre-trial guarantees for defendants**, such as limited opportunities to scrutinise digital evidence and challenge expert testimony; tunnel vision by LEAs; a lack of validation for complex digital forensic tools; and the vulnerable position of suspects/defendants in collecting or challenging electronic evidence. [190] While not directly tied to technology, factors undermining the presumption of innocence also include **'decryption orders,'** which involve the practice of introducing specific legal provisions requiring

189 See G. Raburu, L.Dinga: Legal Issues in Computer Forensics and Digital Evidence Admissibility, IJCSMC, Vol. 9, Issue. 7, July 2020, pp. 86–89. https://ijcsmc.com/docs/papers/July2020/V9I7202021.pdf.

190 See the FORMOBILE Checklist Guidance Document, supra, pp. 29-30. See also Sykova, op. cit., pp. 1–2.

suspects to surrender, under the threat of punishment, passwords or data in an unencrypted format. Additionally, even without formal decryption orders, there is a concern that LEAs engage in **psychological manipulation** to obtain passwords, PINs, or decryption keys and incriminating evidence from suspects/defendants.[191]

In the pre-trial criminal investigation, IT-forensic implications extend beyond the traditional scope of forensics and evidence gathering. While IT-forensic methods involve retrieving information from the internal memory of electronic devices, the electronic data/evidence extracted from these devices is highly volatile, susceptible to easy deletion, alteration, or transfer, thus posing challenges to LEAs in accessing it. In their pursuit of overcoming these challenges in the 'best interests of the investigation,' they may encounter difficulties such as the **proper definition of legal rules governing the collection of electronic data/evidence**, given that the countries mostly rely on general provisions and apply them to electronic evidence.

Another potential challenge for investigators involves correctly identifying the owner of the electronic device to be seized and/or searched. This uncertainty may lead **to improper determinations regarding what part of the data is protected under the right to remain silent or may constitute privileged information between a lawyer and a defendant**. In the worst-case scenario, as previously highlighted, LEAs may resort to explicit actions and practices that raise **concerns about ensuring a fair procedure for suspected/accused persons and increase the risk of wrongful prosecution**.

In the 'analysis phase' of the process, data is inserted into a tool/model, which results in an output that is presented as evidence – evidence that is rarely critically examined nor questioned by the court. Thus, the **burden is effectively placed on the defence to disprove the evidence or to prove that the data is possibly false, when other evidence is lacking**.[192] Further risk factors in terms of reverse of *onus probandi* and violation of fundamental rights include cases where vulnerable suspects and suspects with unconventional behaviour are involved; high profile cases, with increased media/societal pressure to convict and cases where the lines between data gathering, surveillance and investigation techniques are blurred.[193] Drawing from the insights of Stoykova, Mason and Edmond, and Roberts, the FORMOBILE project emphasises two critical factors increasing the risk of miscarriages of justice. Firstly, it points out the close relationship between forensic examiners and law enforcement agencies (LEAs), where examiners are often either directly employed by LEAs or financially dependent on them. Secondly, the project highlights the enthusiasm of LEAs and judges towards novel and unproven science and technology. This enthusiasm can lead to the assumption that digital sources of evidence are functioning properly, even when they may not be.[194]

In the following Subsections, some of the above challenges and threats to the presumption of innocence and other fundamental rights in the pre-trial criminal investigation (i.e. when electronic data is collected, preserved and analysed by LEAs) will be explored in more detail.

191 See the Presumption of innocence and related rights - Professional perspectives, supra, p. 3. See also the INNOCENT Report, supra, pp. 31–32.

192 See the FORMOBILE Checklist Guidance Document, supra, p. 30.

193 See Stoykova, op. cit., pp. 3–5. See also D. M. Risinger, L. C. Risinger: Innocence Is Different: Taking Innocence into Account in Reforming Criminal Procedure. New York Law School Law Review, 56(3), 2012, p. 886.

194 FORMOBILE Checklist Guidance Document, supra, p. 30. See also Stoykova, op. cit., p. 9.

6.1.4.1. 'Decryption orders'

The presumption of innocence places a prohibition on State authorities to use compulsion, imposes a duty to ensure that the burden of proof for establishing the guilt of suspects and accused persons lies with the prosecution, underscores that any doubt regarding guilt benefits the suspect or accused person, and guarantees the right of suspects and accused persons to not incriminate themselves and to remain silent concerning the criminal offence they are suspected or accused of committing. A significant legal issue to be explored with regard to the scope of these principles and rights are their legal implications and consequences when it comes to gathering of electronic data/evidence in pre-trial investigation where, at a first glance, the access to the electronic evidence depends on the will of the suspect/accused to unlock their device via password, PIN, decryption key, or simply their fingerprint or face.[195]

Several EU Member States have introduced the so-called 'decryption orders' in their law, requiring suspects to provide passwords, PINs, fingerprints, face scans, etc. to unblock their electronic device, or data in an unencrypted format. These jurisdictions consider, *inter alia*, that passwords, PINs, decryption keys etc. are not evidence. Therefore, in the view of these jurisdictions, suspects can be asked to hand them over and may not be afforded the protection of the right to remain silent or the right against self-incrimination. They could also be sentenced for refusing to do so. For example, judgements of domestic courts in Belgium and Netherlands illustrate that in these two countries, the use of compulsion to obtain from the suspects information or material other than oral statements (i.e. passwords, PINs, fingerprints, etc.) is in accordance with the law. Ireland and France have introduced legal provisions compelling a suspect to provide authorities with access to an electronic device or to hand over the access key or assist the police in accessing the data in an unencrypted format. Refusing to disclose a passcode to law enforcement is a criminal offence and may be punished with imprisonment. In the case of *Minteh v. France*,[196] the 'decryption orders' introduced by the French legislation are currently under review before the ECtHR.

In contrast to the approach taken by the aforementioned countries, the European Union Agency for Fundamental Rights (FRA) asserts that '*defendants are not obliged to provide evidence incriminating them, such as data contained in electronic devices*.' Accordingly, defendants have no obligation to share data with LEAs, including computer passwords, e-mail passwords, personal identification numbers (PINs) for SIM cards and mobile phones, or, for example, private keys for crypto wallets. These pieces of information enable access to potentially incriminating data.[197] However, in practice, such situations do arise. **Practitioners from several Member States interviewed by FRA revealed that, in practice, LEAs attempt to persuade suspects to provide incriminating evidence through promises or threats**. While most of interviewees, including professionals from Austria, Germany, Italy, and Poland, affirm that defendants are not obligated to provide phone PINs, computer or e-mail passwords, or similar information, some defence lawyers highlighted that, in practice, LEAs occasionally encourage suspects to provide incriminating evidence. In most cases, this encouragement is accompanied by suggestions that such cooperation could lead to shorter proceedings or milder treatment.[198]

The authors of the FRA report suggest that '*Member States should provide systematic guidance and training to ensure that police officers consistently explain to*

195 Criminal Procedure Report, supra, p. 27.

196 ECtHR, *Minteh v. France*, a. No 23624/10.

197 Ibid., p. 13. See also the INNOCENT Report, supra, pp. 31-32.

198 INNOCENT Report, supra, p. 32. See also the Presumption of innocence and related rights – Professional perspectives, supra, pp. 78-79. 'In Austria, for example, a lawyer observes that some defendants, namely those who are innocent, provide their passwords during the first police interrogation. [...] Interviewees in Poland note that, although defendants do not have to disclose their computer passwords or phone PINs, sometimes the police ask them to do so 'off the record', arguing that if they cooperate the proceedings will be shorter. [...]. Similarly, in Lithuania, a police officer describes how the police will often ask suspects to provide evidence voluntarily; if they do not do so, as is their right, the police will employ other means to obtain the evidence, for example through a legally mandated house search. The police officer suggests that the only effect that a defendant's choice to remain silent has on the proceedings is that the process takes longer because of the need to look for evidence. In addition, police officers from Germany indicate that, in practice, they explain to suspects that either they can provide them with their PINs or passwords voluntarily or their devices can be forcibly unlocked, which will take significantly longer and cost money. The police officers report that they present the advantages and disadvantages of both options in an impartial manner and do not think that this puts pressure on suspects. However, most of the other professionals interviewed in Germany perceive such behaviour differently. Prosecutors admit that this behaviour does put pressure on suspects, while a lawyer states that the police often act as though suspects are obliged to provide their passwords. Two other lawyers note that the police sometimes falsely claim that they can obtain a court order for a certain measure or make false promises about a shorter sentence in a potential trial. Similarly, in Italy, a lawyer reports that the police can pressure suspects and

defendants their rights, including the consequences of remaining silent, making a confession, or providing evidence or information that incriminates them.'[199] It appears, however, **that there is no definitive or clear answer in international and EU law, including the case law of the ECtHR and the CJEU, as well as in the legal literature, whether such practices involve (indirect) compulsion and violate the presumption of innocence**.

Regarding the law and practice in countries participating in the INNOCENT project, significant diversity was identified among them. For example, in Bulgaria, there is a distinction between obliging a suspect to 'give' a DNA sample and requiring them to reveal a password. While a suspect can be obliged to provide a DNA sample, this obligation cannot be extended to data such as PINs and passwords, as it would violate their right to remain silent. In Slovenia, the relevant provisions are somewhat mysterious. The Criminal Procedure Act states in Article 219.a that the owner or user of the electronic device must provide access to the device, explanations about its use, and encryption keys or passwords necessary for the investigation's purpose. Refusal to do so may result in a fine of up to three times the average salary in the Republic of Slovenia or imprisonment for a maximum of 10 days, unless the individual is a suspect, an accused person, someone who cannot be heard as a witness, or a person with the right to refuse to testify. However, it is not entirely clear how these provisions are interpreted and implemented in practice. In Croatia, unlike Slovenia, there is a clear legal provision in Article 257 of the Criminal Procedure Act regulating searches, stating that everyone, including a suspect, can be compelled to provide authorities with access to an electronic device. However, this provision is considered *lex imperfecta*, as the wording suggests that a suspect should provide access to the device, yet they must not be punished if they fail to do so.

Instead of passwords and PINs, many people use biometric encryption, such as fingerprints and facial recognition to protect their privacy on their electronic devices. The question whether the right to not incriminate oneself could be extended to a refusal to unlock the mobile device by means of biometrics has been posed as a separate legal issue.

National perspectives on this matter also widely differ, depending on the different interpretations of the *Saunders v. the United Kingdom*. **Some jurisdictions, including the Netherlands, Denmark, Finland, Germany, Lithuania, Norway, and Italy, consider the use of biometrics or facial recognition to unlock a device as non-coercive, viewing it as the use of material having an '*existence independent of the will of the suspect*.' Conversely, Austria, Croatia, Greece, Sweden, Malta, and Slovakia maintain a different stance**. In Sweden, for example, the Parliamentary Ombudsman issued a decision that forcefully taking and using a fingerprint to unlock a mobile device has no legal support. **The third way to deal with this issue is the requirement of a dedicated court warrant. This 'solution' is employed by Belgium, Cyprus, Ireland, Kyrgyzstan, Luxembourg, and Spain**.[200]

To determine whether a suspect might be forced to unlock their device using their fingerprint or face scan, most often the provisions of Directive (EU) 216/343 and the interpretation by the ECtHR of the right to a fair trial under the ECHR are taken into account. According to Article 7(3) of Directive (EU) 216/343, the **scope of the right to not incriminate oneself is limited**. The provisions of this article establish that the exercise of the right to not incriminate oneself is without prejudice to any acts from the competent authorities directed to

accused persons to accept an unauthorised police search by telling them that a public prosecutor will authorise it anyway. One interviewee describes such behaviour as deceptive, as the police have no influence on courts and sentencing.'

199 Ibid., p. 13. See also the INNOCENT Report, supra, pp. 31-32.

200 The Criminal Procedure Report, supra, pp. 54–56.

gather evidence that has been lawfully obtained through the use of legal powers of compulsion and which existed irrespective of the will of the suspected or accused persons. This includes material acquired pursuant to a warrant and material in respect of which there is a legal obligation of retention and production upon request, such as breath, blood and urine samples, and bodily tissue for the purpose of DNA testing. Similarly, as pointed out in Section 4.2 of this Toolkit, the ECtHR stated in *Saunders v. the United Kingdom* that the right to not incriminate oneself is limited, so that '*it does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers and material which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing*'.[201]

In the view of the authors of this Toolkit, there is no straightforward answer to the question at issue. While it can be argued that the use of fingerprints or facial recognition to unlock a device is not considered a coercive measure, but rather use of 'material' that has an existence independent of the will of the suspect, a diametrically different stance is equally legitimate: the suspect or the accused person has consciously and of their own free will decided to secure the access to the electronic device with biometric protection.[202] In *Allan v. the United Kingdom*, the ECtHR held that **the right to remain silent and the privilege against self-incrimination are not only designed to protect against improper compulsion by the authorities and the obtaining of evidence through methods of coercion or oppression, but to protect the freedom of a suspect or an accused person to choose whether they wish to cooperate with the investigators or not**. Hence, if a person does not wish to give statements and, instead, wishes to remain silent (e.g. passive), the right to remain silent and the self-incrimination privilege should protect them from being forced to provide their fingertips, face scan, passwords or PINs required to unlock their devices. **The freedom of choice is undermined when a suspect refuses to cooperate and the authorities use force or deceitful tactics to influence them to act in a way which will result in their incrimination**. Additionally, answering the question as to whether 'decryption orders' targeting biometric protection, as well as passwords and PINs, violate the right to remain silent and/or the right to not incriminate oneself, one can reasonably conclude that from a legal perspective, there is no difference between forcing a suspected or accused person against their free will to supply their fingerprint or password, which leads, or could lead, to incriminating material against them, and forcing them to unwillingly hand over the incriminating material.

Linked to this issue is **an increased number of cases that are being brought to court where a violation of the *nemo tenetur* principle is alleged because the defendant was obliged by law to provide their password to the police or their biometrics were used against their will to unlock a device, thereby granting access to the data**. In one of these cases, decided by the Supreme Court of the Netherlands,[203] the legal issue was whether the investigating officers were authorised to seize the accused's iPhone and gain access by forcing the accused to unlock his iPhone using his fingerprint.[204]

In the first instance, the court stated that for the purpose of ascertaining the truth, it was permitted to investigate seized objects to obtain data for the criminal investigation. The legal basis for such investigation lies in Articles 94-96 of the Dutch Criminal Procedure Code. The Court affirmed that when a phone, for example, is protected by an access code, the investigators are allowed to crack this protection without the cooperation of the suspect. Moreover, a suspect

201 Saunders v. the United Kingdom, supra.

202 See also the various court decisions in the United States, a majority of which consider the protection of electronic devices by fingerprints to fall under the privilege against self-incrimination. J. Hoffer: The Ongoing Legal Battle: Biometrics, 5th Amendment, and Phone Decryption, January 2023, https://medium.com/the-berkeley-table/the-ongoing-legal-battle-biometrics-5th-amendment-and-phone-decryption-8353c6f2f81a.

203 Supreme Court of the Netherlands, 13 October 2020, ECLI:NL:HR:2021:202.

204 See the FORMOBILE Checklist Guidance Document, supra, pp. 22–23.

can even be forced to cooperate by the placing of their thumb onto their iPhone without their permission/cooperation. This is because, in the opinion of the Court, this involves an investigative measure that does not require the active cooperation of the accused, with the fingerprint being obtained with only a very small degree of coercion.[205]

The Court of Cassation and the Supreme Court uphold these arguments. The Supreme Court found that the purpose of unlocking the iPhone, by placing the suspect's thumb on the device, was to secure the data stored or available on it. It refused the argument that Articles 94-96 of the Dutch Criminal Procedure Code do not form a sufficient legal basis for gaining access to a seized object by unlocking it biometrically against the suspect's will using their fingerprint. Furthermore, it struck down the appeal that there was a violation of the *nemo tenetur* principle. The Supreme Court followed the first judge and stated that applying a very small degree of physical coercion in this manner with the aim of biometrically unlocking the smartphone by means of the suspect's fingerprint does not constitute a violation of the *nemo tenetur* principle guaranteed by Article 6 of the ECHR. It considered the seriousness and nature of the suspicions against the suspect, the lack of the accused person's cooperation in unlocking the iPhone, and the justified expectation of the police officers that the iPhone would contain data relevant to the investigation. The Supreme Court believed that a less drastic means of unlocking the iPhone was not available.[206]

6.1.4.2. The right to information and the right to access to a defence lawyer in the context of gathering of electronic evidence

In any pre-trial investigation, including those involving gathering of electronic data/evidence and IT-forensics, the right to be given adequate information about the right to remain silent, the right to not self-incriminate and the right to access to a defence lawyer is of paramount importance for an effective implementation of the right to a fair trial.

LEAs should ensure that suspects are effectively informed about their procedural rights – possibly in both written and oral formats, using accessible language, regardless of whether a defendant is deprived of their liberty – as soon as they are suspected of having committed an offence. When a police officer reads out a suspect's rights, they should make sure that the defendants are able to fully comprehend this information in the time available.[207] To ensure the effective implementation of rights and safeguards for a suspect or accused person during pre-trial investigations involving the seizure of electronic devices, the notice of rights should include information stating that there is no obligation to provide passwords, PINs, etc.[208]

205 Ibid.

206 Ibid.

207 Rights in practice: right to access to a lawyer and procedural rights in criminal and European arrest warrant proceedings, supra, pp. 12, 23.

208 As shown in Subsection 6.1.4.1, this imperative is not followed by countries which introduced 'decryption orders' in their law.

In practice, early access to a defence lawyer is often a key safeguard of these rights.[209] Additionally, with respect to the accused and their counsel, the principle of equality of arms should be carefully considered, taking into account that the prosecution has an advantage when it comes to the possibility of engaging various experts in the examination of the electronic evidence and the request for disclosure of these evidence.

The FRA identified cases where LEAs questioned a person as a witness or 'informally' asked them questions, even when there were plausible reasons for suspecting that person's involvement in a crime. This means that defendants did not receive information about their rights as a suspect and, in particular, the right to remain silent and to not incriminate themselves.[210] This practice is not consistent with police ethics and may cause irreparable damage for the accused person. In accordance with the ethical standards of police work, investigators should eliminate practices of placing defendants under a different procedural, 'pre-suspect', status and therefore of failing to inform them of their rights. In cases involving gathering of electronic data/evidence, the same should be applicable.

LEAs should ensure access to a lawyer before the initial gathering of information from or questioning of suspects, maintaining this access throughout the entire proceedings. This provision should extend to obtaining information from a suspect regarding their electronic devices, passwords, decryption keys, etc., for unlocking these devices. Generally, when a suspect requests the presence of their lawyer, LEAs should postpone gathering information and questioning until the lawyer arrives, refraining from any procedural activities (regarding the acquisition of electronic data/evidence) until legal representation is secured. Suspects and accused persons should be allowed a private conversation with their lawyer, irrespective whether the defendant is deprived of liberty. **If for any reason a defence lawyer is not present – to avoid violations of the informing obligation about the right to remain silent – a video documenting police interrogations can be a key to the protection of a defendant's right to remain silent and to not incriminate themselves**.[211]

Regarding the information disclosed to the defence, the FORMOBILE project emphasises the need for a higher level of transparency than currently provided in most EU legal systems. In many jurisdictions, the defence is typically informed only of the investigation's outcome and granted access solely to evidence included in the case file. **In the context of electronic evidence, presentation of evidence often involves not the original evidence itself but a printout of digital data or written protocols. Even when the defence is given access to a digital copy of evidence extracted from an electronic device, typically through creating a complete copy, there is often a lack of information about the investigative approach to that evidence. While some countries recognise the importance of implementing a standardised process ensuring a clear chain of custody (including timestamping and identification of the individual handling the evidence), the overall approach seems fragmented**. Importantly, few countries in the EU explicitly acknowledge access to this information as an inherent right of the defendant.[212]

In accordance with Article 6(3)(b) of the ECHR, individuals should be guaranteed adequate time and facilities for the preparation of their defence. **During pre-trial investigations, police and prosecution should promptly**

209 Rights in practice: right to access to a lawyer and procedural rights in criminal and European arrest warrant proceedings, supra, p. 12. See also the INNOCENT Report, supra, p. 32.

210 Ibid., pp. 12, 30–31.

211 See ibid., pp. 13, 37. See also the Presumption of innocence and related rights - Professional perspectives, supra, pp. 78–79 and the INNOCENT Report, supra, p. 32.

212 See the Criminal Procedure Report, p. 26.

provide persons suspected or accused of a crime with the data gathered from their seized or unseized mobile devices, or, at least, all data relevant for preparing a proper defence. Although the ECtHR has allowed restrictions to the principle of disclosure of relevant evidence to protect police methods, such limitations must be strictly necessary to be allowed under Article 6 of the ECHR. In general, in terms of the transparency of information disclosed to the defence, the FORMOBILE Project highlights the need for a higher level of transparency than is currently being provided in most legal systems across the EU, even though specific details are yet to be settled in practice.[213]

6.1.4.3. The right to privacy and the protection of personal data in the context of gathering of electronic evidence

According to Article 8 of the ECHR, '*everyone has the right to respect for his private and family life, his home and his correspondence*.' There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the conditions stipulated by the Convention. A somewhat shorter but similar provision can be found in the Charter: '*Everyone has the right to respect for his or her private and family life, home and communications.*'[214] Contrary to the ECHR, the Charter also contains a provision on the protection of personal data. It provides in Article 8 that everyone has the right to the protection of personal data concerning themselves. Such data must be processed fairly for specified purposes and based on the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning themselves, and the right to have it rectified.

The FORMOBILE project has highlighted the challenges associated with gathering and handling electronic evidence, which raise, especially in the realm of IT forensics, significant concerns regarding the protection of privacy, family life, and the confidentiality of correspondence. The wealth of information stored on smartphones and other electronic devices presents difficulties for existing procedural rules and practices, leading to notable gaps in the safeguarding of privacy. Notably, the concern extends beyond the privacy of the suspect, encompassing the privacy of numerous third parties whose data is collected when a LEA accesses a suspect's device. This situation broadens the scope of individuals whose data is processed during an investigation, even if they are not directly implicated. Considering these complexities, there is a pressing need to re-evaluate current approaches within the legal frameworks of Member States.[215]

In general, in pre-trial investigation, electronic data/evidence collection concerns the search of a complex balance between the legitimate interests and duties of the State to persecute crime and guarantee the safety of citizens and their right to (and reasonable expectation of) privacy, as well as the expectation for LEAs to comply with data protection law.

213 Ibid. According to the FORMOBILE, the following questions should be addressed during the investigation: Must all data gathered be accessible to the defence in an electronic format? Must they be informed about all police methods used, the specific (combination of) tools used and the reasoning behind actions taken by investigators? How about problems with the results produced by tools known to the scientific community or to investigators?

214 The Charter of the Fundamental Rights of the European Union, Article 7.

215 See the FORMOBILE Checklist Guidance Document, supra, pp. 29–30.

However, the **right to privacy is not an absolute right**. Pursuant to the second paragraph of Article 8 of the ECHR, it can be subject to limitations that are 'in accordance with the law' and deemed 'necessary in a democratic society.' These limitations may be imposed for reasons such as national security, public safety, economic well-being, disorder or crime prevention, health or morals protection, or safeguarding the rights and freedoms of others. Consequently, concerns regarding privacy may be set aside when it is imperative to maintain societal safety and prevent or investigate crimes. However, any restrictions imposed should be deemed necessary and proportionate to the specific circumstances.

Considering the gathering and handling of electronic evidence, these principles align not only with the Convention, but are also reflected in the EU data protection law, particularly in the Law Enforcement Directive. The Directive emphasises that **data gathering should not be excessive and should not be kept longer than is necessary concerning the objectives of the investigation**, reinforcing the need for a balanced and proportionate approach in safeguarding privacy while addressing law enforcement necessities. These principles are crucial in the context of all investigative measures aimed at gathering evidence from electronic devices and should be explicitly ingrained in the procedural laws of the Member States.[216]

With regards to guaranteeing citizens their right to (and reasonable expectation of) privacy when collecting electronic evidence, the identity of the data owner/originator is of particular importance. **Various jurisdictions employ distinct standards and criteria to balance the privacy rights of suspects and accused individuals. This becomes particularly significant when data acquisition involves witnesses, victims, or other third parties, given that electronic devices contain highly personal information that often does not relate to the respective criminal proceedings**. Therefore, in numerous investigations, it is unnecessary to access elements such as family photos, private correspondence with individuals unrelated to the investigation, intimate or medical details, and the like. A concept tied to this notion is to establish a fundamental domain of private life that investigators should refrain from delving into, unless, of course, that specific aspect of private life is pertinent to the crime under scrutiny. Using forensic software solutions is also crucial, enabling LEAs to extract only the data relevant to the ongoing investigation. While this does not negate the possibility of acquiring all data on a device when warranted, there should be a sense of proportionality to ensure that the investigation of crimes doesn't lead to an unwarranted and excessive intrusion into the privacy of both the defendant and third parties, or, worse yet, devolve into fishing expeditions.[217]

During the pre-trial investigation stage, when acquiring, preserving, and analysing electronic data/evidence from either seized or non-seized electronic devices, it is imperative for investigators and forensic examiners to adhere to proper procedures. This is essential to prevent any infringement on privacy rights and other legal protections. **Forensic examiners should strictly follow the national laws that transpose the provisions of the Law Enforcement Directive, specifying different treatment for data belonging to various categories of data subjects, including witnesses, victims, or suspects/accused**. Additionally, the Directive calls for a clear distinction between data based on information and data based on personal assessment. To ensure accountability and compliance with legal standards throughout the electronic data/evidence handling

216 See ibid., Article 4 and Recital 26. See also the FORMO- BILE Checklist Guidance Document, supra, pp. 29–30.

217 See the FORMOBILE Checklist Guidance Document, supra, pp. 26–27 and the Criminal Procedure Report, supra, p. 28.

process, investigators and forensic examiners must demonstrate that correct practices and processes were employed through the application of the LEAs' standard operating procedures.[218]

In a similar vein, the Information Commissioner's Office has underscored the importance of integrating privacy considerations into the technology employed by LEAs for data extraction. The emphasis lies on designing principles that ensure the investigation aligns with legal obligations. The findings in the Information Commissioner's report[219] not only highlight the requirement for LEAs to restrict the acquisition of unnecessary data, but also stress the need to curtail the further processing of information that exceeds the investigation's intended purposes. Moreover, the report advocates that, moving forward, LEAs should exclusively adopt tools that align with this privacy-centric approach. The right to privacy, it suggests, necessitates a more cautious stance on data collection and processing from electronic devices, discouraging the indiscriminate gathering of all data for subsequent sifting, whether through manual screening or the use of AI and other pre-selection techniques.[220]

The recognition of the necessity for data retention is widespread among LEAs, given that data can be necessary for the purposes of investigation, forensic research, validation of tools and possibly opening of cold cases. However, the data protection law poses a challenge to this concept. **While data must be preserved and archived in a forensically sound manner, any unused data must be deleted. Relevant provisions regarding data storage and deletion in the context of electronic evidence can be found in national criminal procedure legislation, human rights, and data protection law, as well as in the Law Enforcement Directive and in the case law of the ECtHR**.[221]

Article 5 of the Directive states that Member States shall provide for appropriate time limits for the erasure of personal data or for the specific review of the need for storage of personal data. This means that time limits for erasure of personal data are to be found in the different legal acts transposing the directive into national law. Article 16 of the Directive obliges Member States to establish the right to erasure, under specified conditions (i.e. where the processing of personal data is unlawful, or it does not follow the principles relating to processing of special categories of personal data). However, Member States are not precluded from adopting higher standards of protection than those set out by the Directive.[222]

More detailed requirements for data retention and procedures for deletion in national law are required by the ECtHR's case law. In principle, the Court considers the mere storing of data an interference of the right to respect of private life as enshrined in Article 8 of the ECHR. However, such interference may be justified under Article 8(2) ECHR if 'in accordance with the law' and 'necessary in a democratic society'. To assess the justification for interference, the Court instituted a specific test. Generally, the Court does not view data deletion as unduly burdensome for public authorities, even in cases involving non-fully automated databases. To strike a balance between public interests and individual rights, a judicial process is essential, ensuring an impartial review of justifications for data retention. This system should operate based on clear criteria and extend adequate safeguards to individuals seeking the removal of their data, making the opportunity for data deletion tangible and not merely theoretical. Individuals pursuing data deletion should have practical means to challenge the accuracy, retention, and storage of their data. Despite the inclusion of time limits

218 See the FORMOBILE Checklist Guidance Document, supra, pp. 26-27 and 34. The FORMOBILE refers to M. Simonato: Defence rights and the use of information technology in criminal procedure. Revue internationale de droit pénal, 85(1-2), 2014, pp. 291–292 and G. Vaciago, D. Silva Ramalho: Online searches and online surveillance of trojans and other types of malware as means of obtaining evidence in criminal proceedings. Digital Evidence and Electronic Signature Law Review, 13, 2016, pp. 91–93.

219 Information Commissioner's Office, 'Mobile phone data extraction by police forces in England and Wales Investigation report', (ICO, 2020), Version 1.1, https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-inengland-and-wales-v1_1.pdf.

220 See the Criminal Procedure Report, supra, p. 29.

221 See the FORMOBILE Checklist Guidance Document, supra, pp. 49–50.

222 Ibid. See also Directive (EU) 2016/680. The Bulgarian Supreme Administrative Court filed a request for a preliminary ruling to the Court of Justice of the European Union (CJEU), by asking whether Articles 5, 13(29)(b) and 13(3) of the Law Enforcement Directive allow national law which leads to a virtually unrestricted right for authorities to process personal data and whether they allow for the elimination of the data subject's right to restricted processing or erasure. The CJEU ruled that the law Enforcement Directive does not allow to the police for data to be stored and processed indefinitely. The data controller has an obligation to review periodically whether the data is necessary and must grant the data subject their tights when data is no longer necessary to the purpose of processing. See CJEU Judgement of 30 January 2024, C-118/22, ECLI:EU:C:2024:97.

in national legislation, authorities retain the discretion to refuse data deletion and keep it indefinitely if deemed necessary. In such cases, authorities must provide a well-reasoned opinion. Furthermore, individuals should not be left dependent on the discretionary powers of authorities governed by a flexible legal framework. Special protection should be accorded to sensitive categories of data.[223]

CHECKLIST OF KEY POINTS ON E-EVIDENCE IN THE PRE-TRIAL INVESTIGATION (COLLECTION, PRESERVATION AND ANALYSIS OF E-EVIDENCE)

- ☐ In the pre-trial investigation stage, the need to maintain balance between the legitimate interest of the State to investigate and prosecute crimes and the need to safeguard fundamental rights and freedoms guaranteed to individuals is of a paramount importance.
- ☐ Regarding electronic data and evidence, the process during the pre-trial investigation can be divided into several phases, which include *collection*, *preservation* and *analysis* of e-evidence.
- ☐ In the pre-trial criminal investigation, IT-forensic implications extend beyond the traditional scope of forensics and evidence gathering. The early use of technology often compromises the principle of the presumption of innocence. Problems arise from shortcomings in digital forensic practices, inappropriate and inconsistent technology use, outdated procedural guarantees, and issues within the digital forensic practice.
- ☐ The collection phase encompasses pre-collection activities, including preparation, planning, and the examination of the crime scene, as well as various methods employed by LEAs for evidence gathering. LEAs may conduct these activities autonomously, employing methods such as acquisition, seizure, interruption, etc., or in collaboration with telecommunications operators, internet providers, or other private entities.
- ☐ The preservation should be focused on the maintenance of the electronic data to guarantee that irrespective of the time frame the retention process is able to withstand judicial scrutiny (the principles and safeguards applicable must ensure that the evidence withstands the same scrutiny as to admissibility, authenticity and persuasiveness).
- ☐ To ensure the authenticity, integrity and reliability of the data and for the evidence to be accepted at the trial, the maintenance of the *chain of custody* by the investigator(s) is of paramount importance. The chain of custody aims at documenting where, when, why and how certain actions were taken, and by whom (including whether that person was qualified to do so).
- ☐ In the analysis phase of the process, data is inserted in a tool/model, which results in an output, which is presented as evidence, rarely critically examined nor questioned by the court. Thus, effectively the burden is put on the defence to disprove the evidence or to prove that the data is possibly false, when other evidence is lacking.

223 See the FORMOBILE Checklist Guidance Document., supra, p. 51. See also Stoykova, op. cit., p. 4.

- Several EU Member States have introduced so-called 'decryption orders' into their law, requiring suspects to provide passwords, PINs, fingerprints, face scans etc. to unlock their electronic device or data in an unencrypted format. These jurisdictions consider, *inter alia*, that passwords, PINs, decryption keys etc. are not evidence. Therefore, in the view of these jurisdictions, the suspects can be asked to hand them over and do not enjoy the protection under the right to remain silent or the right to not incriminate oneself, and could be sentenced for refusing to do so.
- In contrast to the approach taken by the countries, according to FRA, defendants have no obligation to share data with LEAs, including computer passwords, e-mail passwords, and PINs.
- There is an increased number of cases that are being brought to court where a violation of the *nemo tenetur* principle is alleged because the defendant was obliged by law to provide their password to the police or their biometrics were used against their will to unlock a device, thereby giving access to the data.
- In pre-trial investigations involving the seizure of electronic devices, acquisition of electronic data/evidence, and IT forensics, LEAs should ensure access to a lawyer before the initial gathering of information from or questioning of suspects.
- The wealth of information stored on electronic devices raise, in the realm of IT forensics, significant concerns regarding the protection of privacy, family life, and the confidentiality of correspondence. Notably, the concern extends beyond the privacy of the suspect, encompassing the privacy of numerous third parties whose data is collected when a LEA accesses a suspect's device.

6.1.5. Procedural parties' role in gathering and handling electronic evidence in pre-trial investigation

In the pre-trial stage of criminal proceedings, the procedural roles undertaken by prosecutors, investigating judges, and defence lawyers in the collection and forensic analysis of electronic evidence require thorough consideration. Their responsibilities encompass authorisation, execution, and supervision of the data acquisition, preservation, and analysis processes, underscoring the importance of a comprehensive and responsible approach to these crucial aspects of legal proceedings.

6.1.5.1. Prosecution

Starting with the prosecutors, it is their responsibility to shoulder the initial burden of proof and present the evidence to the court in a suitable manner. **To establish the credibility of the evidence, the prosecution must demonstrate the fact or theory beyond any reasonable doubt. Upholding the presumption of innocence and the principle of *in dubio pro reo*, any doubt that arises should be in favour of the accused.**

> The main duty of the prosecution involves issuing, coordinating, and overseeing pre-trial investigation measures. Prosecutors play a crucial role in guiding investigators through the different phases of the chain of evidence until the court approves the indictment. It is imperative for the prosecution to ensure that investigators, acting as the initial responders, fully comprehend and adhere to the legal and IT-forensic prerequisites necessary for producing trial-ready electronic evidence. Adhering to the general rules of evidence, electronic evidence must satisfy criteria related to authenticity, integrity, admissibility, and persuasiveness.[224]

Ensuring reliability presents an initial challenge. In terms of **authenticity**, electronic evidence aligns with traditional evidence requirements. It is crucial to establish that the evidence is genuine, originating from the claimed source (e.g. the suspect's phone or computer), and that its integrity remains intact, free from deliberate or inadvertent alterations in preceding stages. Subsequently, electronic evidence must be persuasive, signifying both inherent reliability (accuracy, authenticity, and lack of alteration) and the ability to substantiate a given fact or theory.[225] Moreover, for authenticity and **integrity**, a dependable chain of custody is indispensable. It is important to verify the accuracy of the data, confirming the absence of errors or imprecisions, or ensuring that any imprecisions do not compromise its evidentiary value. The potential for bias in reporting should be acknowledged and explicitly addressed. Finally, **admissibility** refers to compliance with applicable laws and regulations, ensuring the court's acceptance of presented evidence. This commonly involves evaluating whether proper procedures were followed during the collection phase.[226]

224 224 Ibid., pp. 36–38.

225 Ibid. The prosecution must articulate why specific electronic data can be trusted to substantiate the alleged fact or theory concerning the suspect. This involves presenting a compelling case for the trustworthiness of the electronic evidence in question.

226 Ibid. The FORMOBIE gives an example of the prosecution relying on location data related to the suspect's phone to establish the suspect presence at the crime scene. It must not only demonstrate the admissibility of this evidence (e.g. that it was obtained through proper legal procedure), but also the authenticity, reliability and integrity of these data. Furthermore, it is essential to elucidate the extent to which this particular piece of data can conclusively prove the suspect's presence at the crime scene. Considerations should be made for scenarios where the suspect may not have had their phone with him/her, and someone else brought the phone to the crime scene. In such cases, addressing the potential divergence from the assumption that the phone's presence equates to the suspect's presence becomes a crucial aspect of the evidentiary analysis.

The activities of the investigators and the prosecution must be initiated based on a written request and grounded in a legal framework provided by national law. In this regard, adhering to the principle of legality is paramount, both at the level of adopting legislation as well as regards its application. **Prior to obtaining electronic data/evidence, LEAs should possess at least a reasonable suspicion of a committed criminal offence. In certain jurisdictions, LEAs and prosecutors are required to secure a court order before commencing an electronic device search and data acquisition. Once initiated, the investigation should adhere to the fundamental rights of suspects/defendants and other involved parties, as outlined in the ECHR and the Charter. In criminal procedures rooted in the inquisitorial tradition, the prosecution is obligated to collect both inculpatory and exculpatory evidence**.[227]

As highlighted in the preceding Sections of this Toolkit, achieving fairness and balance between effective law enforcement and the protection of individual's rights is crucial in conducting investigative actions, ensuring the reliability and admissibility of evidence. **Suspects and accused individuals should be presumed innocent until proven guilty in accordance with the law, placing the burden of proof on the prosecution as an additional safeguard**. Important aspects in the application of the rules related to the presumption of innocence which are related to the investigation, as well as the role of the prosecution, therein concern both the forced unlocking of an unseized mobile device through the biometrics of its user and the sharing of a password, *versus* the right to remain silent and the right to not incriminate oneself. **Depending on national legislation, the presumption of innocence and the right to a fair trial should necessitate oversight by the prosecution, ensuring that LEAs should not compel suspects or accused persons to provide information if they have not expressed their explicit consent, or the authorities have a legal basis or a dedicated judicial order to do so**.[228] When issuing, coordinating, and overseeing pre-trial investigation measures and reporting the evidence to the court, the prosecution should also make sure that investigators, including IT-forensic examiners, comply with privacy and data protection rights.

Finally, but equally significant, to enhance cooperation in cross-border criminal cases, LEAs and prosecutor's offices have access to instruments like the existing Mutual Legal Assistance (MLA) Treaties, the European Investigation Order (EIO), and the newly introduced European Production and Preservation Orders (see Section 6.3 of this Toolkit).

6.1.5.2. Defence Lawyers

Defence lawyers are of key importance for the protection of fundamental rights and procedural guarantees of suspects and accused persons. At the pre-trial stage of criminal proceedings, a defence lawyer must identify the precise nature of the charges against the defendant and develop an effective response strategy. The initial analysis of the prosecution case and the subsequent decision-making process in the pre-trial phase are crucial for all that follows.

227 See the Criminal Procedure Report, supra, pp. 38–39.

228 Ibid.

During the early stages of proceedings, a defence lawyer must establish a relationship with the defendant, analyse the charges and initial evidence and develop a preliminary strategy of the defence case based on the gathered information and legal analysis. They must identify applicable laws and precedents that may be relevant to the case and prepare potential defence submissions (such as motions to suppress evidence, requests for discovery, call defence and expert witnesses for testimony, the potential plea agreements and other pleadings to protect the defendant's rights) that can be filed at this stage of the proceedings. **Defence lawyers should review and assess evidence collected by the prosecution in order to identify weaknesses or inconsistencies and prepare and conduct their own investigation to gather relevant evidence that may challenge the evidence gathered by the prosecution and support the defence's case. Following the findings of their investigation and legal analysis, they should engage in negotiations with the prosecution to explore the possibility of a plea bargain or a resolution that is favourable to the defendant. Representing the defendant during pre-trial hearings, arraignments, and other court proceedings, they should challenge the admissibility of evidence obtained unlawfully and ensure that the defendant's constitutional rights are protected throughout the pre-trial phase**.

The defence lawyers' general tasks and responsibilities listed above should extend to instances involving the seizure of electronic devices, the collection of electronic data by law enforcement agents, and the forensic examination of the seized data. Additionally, **in cases marked by the gathering of electronic evidence, defence lawyers must assume specific responsibilities and tasks to proficiently advocate for the defendants. This entails a thorough familiarity with statutory human rights law, case law, and emerging legal issues pertaining to electronic evidence**. Furthermore, defence lawyers should cultivate a **comprehensive understanding of the technologies involved**, encompassing the nuances of electronic systems, data storage, and IT-forensic methodologies. To fully understand digital evidence and its production, they need to acquire **the skills to evaluate crucial aspects related to the integrity and authenticity of digital evidence**.[229] This foundational knowledge empowers defence lawyers to critically assess and challenge the electronic evidence presented by the prosecution.

During pre-trial proceedings, defence lawyers should **scrutinise the legality of the evidence acquisition, ensuring that it adheres to the fair trial rights, privacy rights, and any other legal protections**. Specifically, defence lawyers are tasked with verifying whether the mandate for acquisition was duly followed. They must examine whether data ownership was clearly established by investigators, especially in cases involving electronic devices with multiple users. They should also ensure that forensic examiners comply with national law, transposing the Law Enforcement Directive. This includes **assessing adherence to provisions necessitating distinct treatment of data belonging to different categories of data subjects (witness, victim, or suspect/accused) and a clear distinction between data based on fact and data based on personal assessment**. Furthermore, defence lawyers should verify the documentation of justifications for data gathering, as well as the rationale applied to the evidence during analysis, including any assumptions made throughout the process. Insufficient individualisation and accuracy in testing could potentially lead to a violation of the presumption of innocence and the right to a fair trial.[230]

229 The FORMOBILE Checklist Guidance Document, supra, p. 8.

230 Ibid., pp. 33–34. FORMOBILE refers to Stoykova, op. cit., p. 13 and Raburu, Dinga, op. cit., p. 7.

Defence lawyers are responsible for **supervising, or in situations where their presence is not feasible, assessing the preservation process**. They must **thoroughly examine the reliability of digital forensics tools and methodologies used by police experts**, addressing any legal ambiguities related to the forensic analysis of obtained data, and scrutinising the interpretation of such data. When necessary, defence lawyers should **articulate alternative interpretations for presentation in court**. This may require the **engagement of qualified and impartial forensic experts** to analyse and interpret electronic evidence in certain instances. If defence lawyers undertake these activities, the prosecution is obligated to provide additional evidence to substantiate their case.[231]

Furthermore, it may be beneficial to **establish the identity of the data examiner and determine whether the data has been independently analysed**. It is essential to inquire whether the analysis was outsourced to a private firm or agency. If the LEAs' examiners cannot be questioned because the analysis was outsourced, a relevant inquiry involves understanding the guarantees in place regarding the quality of the analysis. In essence, defence lawyers should, where necessary, conduct alternative analyses during the pre-trial stage, as national law may restrict such activities at a later stage if the defence has not declared its intention to do so at this initial phase.[232]

FORMOBILE underscores the **lack of standardised practices across jurisdictions regarding the defence's access to and disclosure of electronic material or evidence obtained and analysed through IT-forensics**. Challenges to evidence gathered from electronic devices commonly hinge on police protocols. However, as outlined in Article 7 of Directive (EU) 2012/13 on the right to information in criminal proceedings, access to material evidence in the possession of LEAs should encompass documents, photographs, and audio and video recordings, regardless of their nature—whether they support or oppose the suspect or accused person. Even though the disclosure of electronic evidence is subject to diverse national rules and procedures, it is generally understood that the deletion of evidence by LEAs before the lapse of their designated retention periods may potentially constitute a procedural violation.[233]

As highlighted in previous Sections of this Toolkit, any examination of electronic evidence is likely to contain data that is irrelevant, confidential, and potentially covered by legal privilege. In certain jurisdictions, if investigators encounter data beyond the scope of the investigation, there is an obligation to immediately cease viewing it. There may also be a legal requirement to notify the defence of 'unused material' when the results of examining an electronic device are not presented as evidence in court. In relation to this, it is especially important for a defence lawyer to ascertain, whenever possible, which data or part of the seized data is subject to legal privilege. This **involves identifying data protected under the right to remain silent and information considered privileged between a lawyer and the defendant**. It is equally important to determine whether investigators have appropriately marked such data, enabling the distinction between the start and end of confidential information.[234]

It is crucial for defence lawyers to **scrutinise the chain of custody for electronic evidence, ensuring its alignment with both legal and technical standards**. They must ascertain whether the fair trial rights of the accused, such as the presumption of innocence, the right to remain silent, and the right to not incriminate oneself, as well as the legal framework governing data protection and privacy, were upheld throughout the process.[235] Recognising the

231 FORMOBILE Checklist Guidance Document, supra, p. 38.

232 232 Ibid., pp. 33–34.

233 Ibid., pp. 38, See also the Criminal Procedure Report, supra, pp. 39–40 and the Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges. Council of Europe (DGHRRL), Strasbourg, 2020, pp. 151–153.

234 The FORMOBILE Checklist Guidance Document, p. 34. See also Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges, supra, p. 140.

235 As regards fundamental rights, when it comes to gathering electronic evidence and IT-forensics, all the general principles, as well as international and EU instruments and national provisions on fair trial and privacy rights are applicable. See Criminal Procedure Report, supra, p. 53.

substantial threats that digital forensics poses to the presumption of innocence and the fairness of criminal proceedings, FORMOBILE suggests various strategies for defence lawyers to mitigate these risks. Essentially, they should **actively participate in the preparation stage, gaining an understanding of how data will be processed to safeguard its integrity against the potential of wrongful prosecution and errors**. It is important at this stage to participate and scrutinise the process and to cross-examine the procedure for deriving evidence from the data. As illustrated by the ECtHR's case law, the opportunity to uncover exculpatory data or evidence and scrutinise the LEAs and the prosecution's methods may diminish at later stages, contingent upon national procedural rules.[236]

Finally, before the start of the trial, defence lawyers should pay **attention to the identification and selection of expert witnesses**. These witnesses must possess the expertise to testify on behalf of the defence, providing critical insights into the nuances of electronic evidence and IT-forensic analysis.

The role of defence lawyers in electronic evidence cases remains pivotal in upholding the principles of fairness and justice in criminal proceedings.

6.1.5.3. Investigating Judges

Investigating judges' essential tasks and responsibilities in the pre-trial stage of criminal proceedings include preserving due process, overseeing evidence collection, and laying the groundwork for fair and just criminal trials. As key architects in the construction of a just criminal investigation, they are responsible for ensuring that the rights of the accused are protected, that evidence is obtained lawfully, and that all investigative actions align with legal standards. They must record all actions taken, decisions made, and evidence collected, ensuring transparency and accountability throughout the pre-trial stage.

Investigating judges provide legal oversight by authorising investigative measures such as searches, seizures and wiretaps with issuing adequate judicial orders, although in certain jurisdictions this may be the task of the prosecutors. Their role is to assess the necessity and proportionality of these actions, striking a balance between the need for evidence and the protection of individual rights. While their tasks may vary among national jurisdictions, investigating judges act as coordinators, overseeing and directing the efforts of LEAs and investigators. This involves safeguarding the privacy and rights of individuals under investigation and ensuring that surveillance measures are proportionate and that any infringement on privacy is justified by legal necessity.

Investigating judges may conduct interrogations and examinations of witnesses during the pre-trial stage. This enables them to gather first-hand information, assess credibility, and ascertain the facts surrounding the alleged criminal activity. They are also tasked with making decisions regarding the detention or release of the accused. This requires a careful consideration of factors such as

236 See the FORMOBILE Checklist Guidance Document, supra, pp. 30–31.

flight risk, potential harm to the community, and the likelihood of interference with the investigation.

Finally, an essential task of investigation judges is the evaluation of collected evidence. They must assess the admissibility, relevance, and reliability of evidence to determine its probative value in the impending trial. Based on the evidence and investigative findings, investigating judges may decide to dismiss the case or recommend formal charges.

General aspects of the role of investigating judges in pre-trial investigations, as described above, are reflected in criminal cases involving the seizure of electronic devices, the acquisition of electronic data/evidence and IT forensics. In general terms, investigating judges play a crucial role in orchestrating a delicate balance between leveraging technological tools and preserving the fair trial and privacy rights of the suspects and accused persons.

As criminal proceedings move into the trial phase, the leading role shifts to the court and the trial judges. While they may decide to initiate additional investigations to generate new electronic evidence, their crucial role is to assess the lawfulness, authenticity and admissibility of electronic evidence or to involve court experts and expert witnesses to evaluate the evidence if/when necessary. The role of judges at the trial stage of criminal proceeding will be explored in the next Section.

CHECKLIST OF KEY POINTS ON PROCEDURAL PARTIES' ROLE

- ☐ The procedural roles undertaken by prosecutors, investigating judges, and defence lawyers in the collection and forensic analysis of electronic evidence require thorough consideration.
- ☐ The primary responsibility of the prosecution includes issuing, coordinating, and overseeing pre-trial investigation measures, thereby playing a crucial role in guiding investigators through various phases of the electronic evidence chain. Given that suspects and accused individuals should be presumed innocent until proven guilty in accordance with the law, the burden of proof is placed on the prosecution. They are obligated to collect both inculpatory and exculpatory electronic evidence. Through supervision, they must ensure that LEAs do not compel suspects or accused persons to provide information in cases where they have not expressed their explicit consent, unless the authorities have a legal basis or a dedicated judicial order to do so. They must present clear and precise reports produced by forensic experts and other documentation to support their case. Reports, as well as prosecutors, must explain the relevance of the electronic evidence, its credibility (authenticity, accuracy, reliability), admissibility and probative value. The potential issue of bias in reporting should be acknowledged and addressed explicitly. The prosecution is obligated to collect both inculpatory and exculpatory electronic evidence.

- The role of defence lawyers in electronic evidence cases is pivotal in upholding the principles of fairness and justice in criminal proceedings. Defence lawyers should request the disclosure of and access to electronic material or evidence obtained and analysed through IT-forensics and, later, critically assess and challenge the electronic evidence presented by the prosecution. Their general tasks and responsibilities during the pre-trial investigation should extend to instances involving the seizure of electronic devices, the collection of electronic data by law enforcement agents, and the forensic examination of the seized data. In addition to their legal knowledge, defence lawyers should cultivate a comprehensive understanding of the technologies involved. They should scrutinise the chain of custody for electronic evidence, ensuring its alignment with both legal and technical standards. They should establish the identity of the data examiner and determine whether the data is independently analysed. It is essential to inquire as to whether the analysis was outsourced. Furthermore, they should identify data protected under the right to remain silent and information considered privileged between a lawyer and the defendant, as well as to determine whether investigators have labelled such data appropriately. They should consider that the opportunity to uncover exculpatory data or evidence and scrutinise the LEAs and prosecution's methods may diminish at later stages. Before the start of the trial, they should pay heed to the identification and selection of expert witnesses.
- In criminal cases involving the seizure of electronic devices, the acquisition of electronic data/evidence and IT forensics, investigating judges should strive to ensure a delicate balance between leveraging technological tools and preserving the fair trial and privacy rights of the suspects and accused persons. When authorising investigative measures, such as searches and seizures of electronic devices, their role is to assess the necessity and proportionality of these actions, striking a balance between the need for evidence and the protection of individual rights.

6.2. E-EVIDENCE AT TRIAL: JUDICIAL ASSESSMENT AND ADMISSIBILITY OF ELECTRONIC EVIDENCE

6.2.1. Common EU Rules on Admissibility of Evidence

Admissibility of evidence is not only a technical rule but also often connected to the main constitutional principles of a national order, such as prohibition of torture, fair trial, right to a fair trial. It reflects the relationship of a society to certain moral values transformed into law, and the balance that society deems acceptable between security and the suspect's rights. Admissibility covers two aspects, namely, the non-use of certain evidence during trial, as well as the exclusionary rule, which involves excluding evidence from the file. This exclusion may be essential to prevent trial judges from being contaminated with inadmissible evidence. In this regard, a two-fold approach in Europe is observed, namely legal systems strictly filtering the information to be admitted at trial (so-called 'controlled systems') and legal systems leaving it to the judge to assess whether it is appropriate to disregard illegal evidence ('free proof systems').237 Furthermore, inadmissible evidence has the tendency to lead to other evidence, thereby raising the question of how it affected (contaminated) further gathered evidence, and whether certain events interrupted such a chain – this is the 'fruit of the poisonous tree'[238] doctrine, including exemptions to the exclusionary rule (for example, exigent circumstances, security exemption, inevitable discovery, etc.).

Regarding these issues, EU Member States offer a wide array of responses and systems, without a unified EU approach in existence.[239] Although Article 82(2)(a) of the TFEU identifies the issue of admissibility as a domain within the EU's competence in criminal law, this has not led to the creation of an EU legislative text, with the gathering and use of evidence still being governed by the domestic law of the Member States concerned (the *forum regit actum* principle).[240] An attempt to use the 'free circulation theory' ('goods theory') of evidence was also rejected in Regulation (EU) 2017/1939 on the European Public Prosecutor's Office.[241] Only certain initial steps are evident in certain legislative instruments and Court of Justice of the European Union (CJEU) judgments. For instance, Directive 2013/48/EU on the right to access to a lawyer refers in Article 12(2) to 'rights of the defence and the fairness of the proceedings' concerning admissibility. A similar approach is replicated in Article 14(7) of the EIO Directive, Article 10(2) of Directive (EU) 2016/343 on the presumption of innocence, as well as in Article 18(5) of the Regulation (EU) 2023/1543 on European Production and Preservation Orders for electronic evidence. Moreover, the CJEU has advanced further on the issue of data retention and mandated that a court or another independent authority must authorise access to traffic data. It also requires an adversarial procedure for assessing such evidence.[242] However, any future common EU admissibility rules should be based on high standards, not to cause unnecessary 'solange' debates[243] in view of possible conflicts between EU and national constitutional law.[244]

237 B. Garamvölgyi et al., eucrim, No 3/2020, pp. 201-208, https://eucrim.eu/media/issue/pdf/eucrim_issue_2020-03.pdf.

238 See U.S. Supreme Court, *Silverthorne Lumber Co. v. United States*, 251 U.S. 385 (1920); and *Nardone v. United States*, 308 U.S. 338 (1939). See also S. C. Thaman: 'Fruits of the Poisonous Tree in Comparative Law', Southwestern Journal of International Law, 2010, v. 16, pp. 333–384.

239 For example, see the reasoning for the ELI proposal on the draft Directive on mutual admissibility of evidence and electronic evidence in criminal proceedings, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU-.pdf. However, the proposal does not address certain issues, like the mentioned fruit of the poisonous tree doctrine, and raises questions in view of a relative approach to certain rights (for example, it does not explicitly exclude the suspect from being forced to provide passwords).

240 See, for example, S. Allegrezza, Critical Remarks on the Green Paper on Obtaining Evidence in Criminal Matters from one Member State to another and Securing its Admissibility, Zeitschrift für Internationale Strafrechts- dogmatik (ZIS), No 9/2010, pp. 569–579; G. Vermeulen, Free gathering and movement of evidence in criminal matters in the EU. Thinking beyond borders, striving for balance, in search of coherence, Maklu 2011, p. 45–47; S. C. Thaman, Exclusionary Rules in Comparative Law, 2013; M. Kusak, Mutual admissibility of evidence in criminal matters in the EU, A study of telephone tapping and house search, Maklu, Antwerpen, 2016, pp. 29–34; M. Kusak, Common EU Minimum Standards for Enhancing Mutual Admissibility of Evidence Gathered in Criminal Matters, European Journal on Criminal Policy and Research, Springer, 2017; M. Kusak, Mutual admissibility of evidence and the European Investigation Order: aspirations lost in reality, ERA Forum. Journal of the Academy of European Law, Vol. 19, No 3, p. 391–401, https://doi.org/10.1007/s12027-018-0537-0.

241 Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office (COM(2013) 534), Article 30(1), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex-%3A52013PC0534.

242 CJEU, case C-746/18, H.K., as regards the Estonian system of data retention.

Therefore, **the primary common criteria regarding the admissibility of evidence are still grounded in the requirements set forth by the ECHR and the judgments of the ECtHR**. In this context, clear standards are established concerning the prohibition of evidence obtained through torture, inhuman and degrading treatment, as outlined in Article 3 of the ECHR.[245] However, the situation becomes less clear regarding violations of fair trial guarantees (Article 6 of the ECHR), such as the privilege against self-incrimination or right to privacy (Article 8 of the ECHR). In these instances, the court applies a balancing test focused on the overall fairness of the proceedings (see also Section 5 of this Toolkit). This test primarily involves evaluating the nature of the violation, the possibility for the defence to challenge the authenticity and use of evidence, and the quality of evidence itself.[246] Additionally, regarding the privilege against self-incrimination, the court occasionally invoked the concept of 'public interest'.[247] Some guidance is also provided regarding the access of case material by the defence in accordance with points (b) and (c) of Article (6)(3) of the ECHR referring to right to defence, including adequate time and facilities for the preparation of defence, and the right to defend themselves in person or through legal assistance of their own choosing, as well as the right to an adversarial procedure and equality of arms.[248] In addition to this, despite case law distinguishing between testimonial and non-testimonial evidence in the context of applying the privilege against self-incrimination,[249] Member States' interpretations significantly vary, particularly concerning the compulsion for suspects to provide electronic passwords. Thus, even common minimum ECtHR standards offer only limited guidance in these matters.

6.2.2. Judicial Assessment of Electronic Evidence

There is **no single system of judicial deliberations across different jurisdictions**, especially in view of the presentation of legal argumentation.[250] Furthermore, different systems have a varying relationship between the principle of **free judicial assessment** - as a main feature of modern criminal procedure - and certain **formal evidence rules**. Such formal rules may relate to the automatic inadmissibility of certain types of evidence, for example, court authorisation for accessing traffic and content data, specific storage deadlines, limitations to certain criminal offences, etc. A violation of any of these requirements can result in the *ex lege* inadmissibility of such evidence.[251] At the same time, judicial assessment represents one phase in the **life cycle of electronic evidence**, encompassing collection, preservation, analysis, application (assessment), and the transfer and exchange of electronic evidence (*supra*). The term 'electronic/digital evidence' is extremely broad,[252] meaning that each forensic approach is influenced by the type of digital evidence, the target digital device, and the electronic environment. A procedure for extracting digital evidence from a mobile device is different from a procedure for extracting digital evidence from a hard drive.[253] Moreover, the assessment of traffic data provided to law enforcement through duly secure channels by the provider under a standardised procedure significantly differs from assessing electronic evidence gathered through bulk data interception and extraction by specific keywords. Additionally, some electronic evidence requires the help of an expert witness, while other evidence does not.

243 See in that regard A. Erbeznik, A. Erbežnik: EU Criminal Law and the Way Forward in the Case of the Functioning of the EPPO, Hrvatski ljetopis za kaznene zna- nosti i praksu (Zagreb), vol. 27, broj 1/2020, str. 55–77.

244 See in that regard an academic proposal, ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings, supra. In the proposal there is a specific Chapter III (Articles 7 to 9). In Article 9, the use of coercion to get access is in principle prohibited, unless it is proportionate and based on a judicial warrant. However, it should be clarified that coercion against the suspect to access electronic storage is never permissible.

245 ECtHR, *Gäfgen v. Germany*, No 22978/05, judgment of 1 June 2010.

246 See, for example, ECtHR, *Schenk v. Switzerland*, a. No 10862/84, 12 July 1988, or *Khan v. United Kingdom*, a. No 35394/97, judgment of 12 May 2000. See also J. McBride: The case law of the European Court of Human Rights on Evidentiary standard in criminal proceedings, Council of Europe, 2018, https://rm.coe.int/council-of-europe-georgia-european-court-of-human-rights-case-study-ev/16807823c3.

247 *Jalloh v. Germany*, supra.

248 For example, ECtHR, *Moiseyev v. Russia*, a. No 62936/00, judgment of 9 October 2008; *Natunen v. Finland*, a. No 21022/04, judgment of 31 March 2009; *Van Wesenbeeck v. Belgium*, a. No 67496/10 and 52936/12, judgment of 23 May 2017; *Sigurður Einarsson and others v. Iceland*, a. No 39757/15, judgment of 4 June 2019.

249 *Saunders v. UK*, supra. See also Minteh v. France, supra. See, also ECtHR, *Yüksel Yalçınkaya v. Türkiye,* a. No 15669/20, judgment of 26 September 2003, whereby Turkish authorities considered and convicted on terror- ism charges anybody who used a specific communication application called Bylock, but refused to provide to the suspect a copy of the ByLock data pertaining to his alleged use of that application.

250 M. Lasser: Judicial Deliberations, Oxford, 2004.

251 See, for example, Article 154 of the Slovenian Criminal Procedural Act regarding, *inter alia*, formal evidentiary rules on admissibility in view of traffic data.

252 For example, in the ELI proposal of a draft directive on admissibility (supra) they define it as 'any data or information generated, stored,

transmitted or otherwise processed in electronic form to be used to prove a fact in criminal proceedings'. See also the Chapter on the definitions above.

253 A. Antwi-Boasiako, H. Venter: A Model for Digital Evidence Admissibility Assessment. 13th IFIP International Conference on Digital Forensics (DigitalForensics), Jan 2017, Orlando, FL, United States, pp. 23–38.

254 See, for example, Slovenian Constitution Court, case No Up- 1006/13, 9 June 2016, regarding a flawed court authorisation for a house search, and case No Up-326/14, 6 December 2017, regarding a flawed court authorisation for a secret surveillance measure. See also ECtHR, *Dragojević v. Croatia*, a. No 68955/11, judgment of 15 January 2015, para. 95 regarding secret surveillance and interception of communications. The court stated: 'In the instant case the four secret surveillance orders issued by the investigating judge of the Zagreb County Court in respect of the applicant were essentially based only on a statement referring to the existence of the OSCOC's request for the use of secret surveillance and the statutory phrase that 'the investigation could not be conducted by other means or that it would be extremely difficult' (see paras 9, 11, 13 and 17 above). No actual details were provided based on the specific facts of the case and particular circumstances indicating a probable cause to believe that the offences had been committed and that the investigation could not be conducted by other, less intrusive, means.'

255 See, for example, Slovenian Constitution Court, case No U-I- 144/19, 6 July 2023, regarding the unconstitutional provisions of Articles 149.b and 149.c of the Criminal Procedure Act referring to traffic data. See also M. Zubik et al.: European Constitutional Courts towards Data Retention Laws, 2021. The authors explore a variety of national constitutional courts' decisions on the illegality of their national data retention systems.

256 For example, ECtHR, *Iordachi and Others v. Moldova*, a. No 25198/02, judgment of 10 February 2009, regarding the secret surveillance legislative provisions.

257 Antwi-Boasiako and Venter, op. cit., p. 27.

258 ELI draft directive on admissibility of evidence, supra, Article 7(1). See also Article 8 (Rules on electronic evidence and forensic standards).

259 ELI draft directive on admissibility of evidence, supra, Article 7(4).

260 Antwi-Boasiako, Venter, op. cit., p.34.

Regardless of such differences, there are some **core elements to consider when assessing the admissibility of electronic evidence**, such as **legality** and **legal authorisation**, **relevance**, **authenticity**, **integrity**, and **reliability**. Moreover, the principles of legality and judicial authorisation play a significant role, as the collection of electronic evidence often involves an encroachment on the right to privacy, sometimes without prior notification of the affected person (for example, requests for traffic or content data directly from the provider). In this context, only at the trial phase does the defence have a real possibility to oppose the data (for example, if the initial authorisation was flawed without an adequate explanation).[254]

Often, the legal basis itself may also be constitutionally flawed[255] and in violation of the ECHR.[256] Some of these elements encompass adherence to a 'chain of custody', namely tracking the movement of evidence from the crime scene all the way through the investigation chain to the courtroom, given the high volatility of certain electronic data. In assessing the admissibility of electronic evidence, an interplay often occurs between legal requirements and technical standards – technical and legal requirements that impact each other.[257] Consequently, electronic evidence in criminal proceedings shall only be used if:

a. the evidence at the time of its use **corresponds to the State in which it was obtained**;
b. the evidence at the time of its use **corresponds to the full extent to the evidence at the time it was obtained**; and
c. the evidence was **sufficiently protected against falsification and manipulatio**n in the period between its obtention and its use (such as access logs).[258]

Therefore, it is of utmost importance that the **defendant has the right to access the full extent of the electronic evidence** and to the report prepared by qualified IT experts, to challenge the chain of custody, the results of the analysis or its interpretation, and also to challenge the conclusions in the expert opinion. Furthermore, it should also be considered how far it is necessary to grant the defendant the right to request the use of machine-learning technology or predictive coding when the full review or the keyword search of documents is not suitable for an accurate assessment of the evidence, to respect their right to defence.[259] Based on the aforementioned reasoning, a possible model on admissibility of electronic evidence could encompass three phases, namely an **assessment phase** comprising of a legality assessment of the order, a **consideration phase** comprising of an assessment of technical standards (mainly chain of custody as its core), and a **determination phase** comprised of assessing the weight of the evidence.[260] However, a specific judicial assessment is needed for cross-border electronic evidence in general and inside the EU.

6.2.3. Admissibility assessment of cross-border evidence

The question of the admissibility of evidence obtained abroad is a complex legal issue, reflecting the challenges associated with foreign requests. The issue of admissibility of evidence is directly **tied to the fundamental rights of the accused in criminal proceedings**, and being often **a constitutional matter** as well.[261] Furthermore, with increasing cross-border cooperation, there is a **risk of 'forum shopping'**, where systems with minimal safeguards are sought to obtain evidence, which is then transferred to another country. Simultaneously, there is a danger of importing foreign anomalies into one's own system (for instance, the absence of judicial orders in some Member States for certain electronic evidence). In practice, in terms of cross-border evidence, questions often arise about the nature of the body that obtained the evidence abroad, the territorial applicability of the national constitutional rules of the State where evidence is transferred to, and on effective legal remedies. Three different approaches to the question of cross-border evidence are possible:

a. mutual recognition of evidence (commodity theory);
b. adherence to the provisions of national criminal procedure; or
c. **admission of cross-border evidence under the condition of respecting constitutional and international principles for protecting individual rights in criminal proceedings**.[262]

Solutions (a) and (b) represent unrealistic extremes, with only solution (c) appearing as reasonably acceptable.

The issue of **asymmetry between ordering** bodies for certain measures in the different Member States is one of the fundamental issues in cross-border legal assistance and mutual recognition, raising the question of requests from bodies that are not judicial authorities. It has already been shown that instruments at the level of the CoE and the EU leave the determination of a 'judicial body' to the discretion of each State. To address this issue, EU instruments introduced a special validation procedure by a prosecutor or court in the issuing State, where the asymmetry between Member States exists, and the involvement of a court authority in the executing State, such as in the European Investigation Order.[263] However, this did not fully solve the issue of the different nature and prerogatives of prosecutors in Member States. In terms of admissibility of evidence, including electronic evidence, it is considered problematic to automatically accept evidence gathered by a body that is not a court when a national constitution requires a court order. **Court authorisation for certain invasive measures provides guarantees against a possible risk of abuse**. Consequently, in most States, measures such as intrusions into communications generally require court authorisation. In the era of modern technology, the internet, and hence new modern technological possibilities available to law enforcement, the demand for a court authorisation is becoming increasingly important for effective protection of expected privacy. Such authorisation and control must not be mere formalism, but an actual substantive critical evaluation conducted within a reasonable time frame.

In this regard, some differentiate between cross-border evidence gathered upon request and evidence based on spontaneous exchange, regarding the territorial applicability of national constitutional rules.[264] This differentiation; however, seems artificial, **as national constitutional safeguards**

261 A. Erbežnik: Mutual Recognition in EU Criminal Law and Its Effects on the Role of a National Judge, in N. Peršak et al., Legitimacy and Trust in Criminal Law, Policy and Justice, Ashgate, 2014. See also Erbežnik, Dežman, op. cit., pp. 284–289.

262 S. Alegrezza: Critical Remarks on the Green Paper on Obtaining Evidence in Criminal Matters from one Member State to another and Securing its Admissibility, Zeitschrift für Internationale Strafrechtsdogmatik, Vol. 5, No 9/2010, pp. 569–579.

263 Directive 2014/41/EU, Article 2.

264 See the Encrochat issue pending before the CJEU, case C-670/22 whereby electronic evidence was transferred from France to Germany and used, although such evidence could not have been obtained in Germany. See also T. Wahl: Encrochat Turns into a Case for the CJEU, eucrim, No 3/2022, pp. 197-198; R. Stoykova: Encrochat: The hacker with a warrant and fair trials?, Forensic Science International: Digital Investigation, Vol. 46, 2023, https://doi.org/10.1016/j.fsidi.2023.301602.

265 See also the ELI draft directive on admissibility of evidence, supra, Article 4(1). 'Member States shall ensure that evidence obtained in compliance with lex loci shall be admissible in criminal proceedings of the forum State unless it infringes fundamental constitutional principles of the forum State.'

266 For example, the Slovenian Constitutional Court in case No Up-127/16, January 20, 2022, stated: 'When transferring evidence from abroad into the Slovenian legal system, a distinction must be made between two acts: obtaining evidence abroad and using evidence in the Slovenian legal system. [...] With the acquisition of evidence in the framework of an investigation carried out by foreign law enforcement agencies abroad outside the territorial validity of the Slovenian Constitution and without the participation or initiative of Slovenian law enforcement agencies, the provisions of the Slovenian Constitution cannot be violated. However, the fundamental constitutional procedural guarantees of the accused, provided by Articles 22, 23, and 29 of the Constitution, must be respected when using such

regarding criminal procedures apply.[265] A different understanding would also mean a violation of the principle of equality before the law. However, the main question is what the national constitutional fundamentals regarding the assessment of evidence gathered abroad are. One cannot impose its own constitutional provisions and the national criminal procedure on other countries. For example, in the case of a catalogue offence limitation, it is not necessary for both countries to list identical offences if both countries consider proportionality in implementing such measures. Such constitutional obligations could refer mainly to certain procedural obligation to respect the rights of the defence,[266] or to provide an efficient legal remedy.[267] Given this, admissibility of evidence gathered abroad should consider four levels of cascading verification:

- respect for the rules in the country of acquisition;
- the minimum standards of the ECHR;
- the minimum standards of the EU (EU Charter and directives on the rights of the accused);
- **possible higher national constitutional standards**.[268]

evidence in a specific criminal proceeding in the Republic of Slovenia, i.e. when transferring such evidence into the Slovenian legal system. However, this does not mean that investigative actions carried out abroad must be strictly judged in terms of the Slovenian Constitution. The inability to use evidence from abroad merely because the manner of its acquisition (which could otherwise be in accordance with a foreign Constitution) did not meet the fundamental procedural guarantees of the Slovenian Constitution would result in the ineffectiveness of criminal prosecution before Slovenian courts. This would violate the positive duty of the State to ensure the safety of persons on its territory (Article 34 of the Constitution). […] The Constitutional Court deemed that the right to equality of arms in the specific case was ensured by the court checking whether the constitutional procedural guarantees of the Italian Constitution protect against arbitrary police interventions in a comparable way as the Slovenian Constitution, whether these guarantees were observed in obtaining the evidence, whether there was a statutory basis for the intervention, and whether the intervention was approved by the competent judicial authority.'

267 See Italian Supreme Court, Case No 44154/23, 7 November 2023, https://canestrinilex.com/en/readings/legality-check-of-skyecc-evidence-is-mandatory-ita-supreme-court-4415423. In the system outlined by the EIO Directive, for the acquisition of the results of an interception already carried out abroad, it is not sufficient that such evidence has been authorised by a judge of a Member State in compliance with the legislation of that State, but there is a need for control which can only be entrusted to the national judge of the issuing State on the admissibility and use of the evidence itself (the interception) according to Italian law.

268 This test is taken from A. Erbežnik, International Encyclopaedia of Laws, EU Criminal Law, Kluwer, 2024.

CJEU, Case C-670, Staatsanwaltschaft Berlin (EncroChat)

1. Interpretation of the concept of 'issuing authority' under Article 6(1) of Directive 2014/41, 1 in conjunction with Article 2(c) thereof:

(a) Must a European Investigation Order ('EIO') for obtaining evidence already located in the executing State (*in casu*: France) be issued by a judge where, under the law of the issuing State (*in casu*: Germany), the underlying gathering of evidence would have had to be ordered by a judge in a similar domestic case?

(b) In the alternative, is that the case at least where the executing State carried out the underlying measure on the territory of the issuing State with the aim of subsequently making the data gathered available to the investigating authorities in the issuing State, which are interested in the data for the purposes of criminal prosecution?

(c) Does an EIO for obtaining evidence always have to be issued by a judge (or an independent authority not involved in criminal investigations), irrespective of the national rules of jurisdiction of the issuing State, where the measure entails serious interference with high-ranking fundamental rights?

2. Interpretation of Article 6(1)(a) of Directive 2014/41:

(a) Does Article 6(1)(a) of Directive 2014/41 preclude an EIO for the transmission of data already available in the executing State (France), obtained from the interception of telecommunications, in particular traffic and location data and recordings of the content of communications, where the interception carried out by the executing State covered all the users subscribed to a communications service, the EIO seeks the transmission of the data of all terminal devices used on the territory of the issuing State and there was no concrete evidence of the commission of serious criminal offences by those individual users either when the interception measure was ordered and carried out or when the EIO was issued?

(b) Does Article 6(1)(a) of Directive 2014/41 preclude such an EIO where the integrity of the data gathered by the interception measure cannot be verified by the authorities in the executing State by reason of blanket secrecy?

3. Interpretation of Article 6(1)(b) of Directive 2014/41:

(a) Does Article 6(1)(b) of Directive 2014/41 preclude an EIO for the transmission of telecommunications data already available in the executing State (France) where the executing State's interception measure underlying the gathering of data would have been impermissible under the law of the issuing State (Germany) in a similar domestic case?

(b) In the alternative: does this apply in any event where the executing State carried out the interception on the territory of the issuing State and in its interest?

4. Interpretation of Article 31(1) and (3) of Directive 2014/41: (a) Does a measure entailing the infiltration of terminal devices for the purpose of gathering traffic, location and communication data of an internet-based communication service constitute interception of telecommunications within the meaning of Article 31 of Directive 2014/41? (b) Must the notification under Article 31(1) of Directive 2014/41 always be addressed to a judge, or is that the case at least where the measure planned by the intercepting State (France) could be ordered only by a judge under the law of the notified State (Germany) in a similar domestic case? (c) In so far as Article 31 of Directive 2014/41 also serves to protect the individual telecommunications users concerned, does that protection also extend to the use of the data for criminal prosecution in the notified State (Germany) and, if so, is that purpose of equal value to the further purpose of protecting the sovereignty of the notified Member State?
5. Legal consequences of obtaining evidence in a manner contrary to EU law: (a) In the case where evidence is obtained by means of an EIO which is contrary to EU law, can a prohibition on the use of evidence arise directly from the principle of effectiveness under EU law? (b) In the case where evidence is obtained by means of an EIO which is contrary to EU law, does the principle of equivalence under EU law lead to a prohibition on the use of evidence where the measure underlying the gathering of evidence in the executing State should not have been ordered in a similar domestic case in the issuing State and the evidence obtained by means of such an unlawful domestic measure could not be used under the law of the issuing State? (c) Is it contrary to EU law, with regard in particular the principle of effectiveness, if the use in criminal proceedings of evidence, the obtaining of which was contrary to EU law precisely because there was no suspicion of an offence, is justified in a balancing of interests by the seriousness of the offences which first became known through the analysis of the evidence? (d) In the alternative: does it follow from EU law, particularly the principle of effectiveness, that infringements of EU law in the obtaining of evidence in national criminal proceedings cannot remain completely without consequence, even in the case of serious criminal offences, and must therefore be considered in favour of the accused person at least when assessing evidence or determining the sentence?

Table 3: CJEU, Case C-670, Staatsanwaltschaft Berlin (EncroChat)

CHECKLIST OF KEY POINTS

- ☐ Before sending a request to another Member State, check any possible procedural differences between your national system and executing State.
- ☐ Follow the minimum criteria set out by the CJEU for meta/traffic data.
- ☐ When receiving evidence gathered abroad, do not reject it solely on the ground that was gathered abroad. Do not automatically accept it, but ensure to check the fundamental rights from international, EU law and your constitution (see the four-element test above).
- ☐ Do not transplant your national rules onto another system. Apply only the fundamental constitutional safeguards of your system in view of the electronic evidence gathered abroad.
- ☐ Focus on an overall data category (for example, content communication data in transfer) instead of the specific investigative measure applied abroad – Member States use various methods to collect electronic data, and these may not be compatible with your domestic law.

6.3. CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE: EU E-EVIDENCE SYSTEMS

Systems for cross-border access to and exchange of electronic evidence are founded on two distinct principles. On one hand, there is the **Mutual Legal Assistance (MLA) approach**, which relies on traditional mutual legal assistance requests. This approach features broad grounds for rejection and is grounded in the CoE and EU MLA conventions. On the other hand, there is the **mutual recognition approach** of EU law instruments (including framework decisions, directives, and regulations). This approach involves cross-border orders that offer limited or no options for the executing State to respond. Following the overview of the legal frameworks provided in Section 3, this Section focuses on the systems for cross-border access to electronic evidence in the EU. We will focus on the main aspects of the EU system for gathering of electronic evidence, including their application scope, types of electronic data covered, conditions for issuance, obligations of the ordering and executing States, grounds for non-recognition, legal remedies, and issues related to admissibility.[269] After presenting each system, we will offer a set of recommendations (checklists of key points) for practitioners. These recommendations will highlight specific considerations to keep in mind when using these instruments. The discussion of these systems is essential to understand the horizontal approach of EU criminal law instruments, especially considering the opt-in option for Ireland and Denmark's non-participation in the Justice and Home Affairs (JHA) area post-Lisbon Treaty. This situation requires that these two Member States continue to use the classical MLA approach, whereas the new e-evidence approach applies to other Member States.[270]

6.3.1. European Investigation Order (EIO)

The general EU system for the collection of cross-border evidence was established by **Directive 2014/41/EU on the European Investigation Order (EIO)**. The system is based on a classical understanding of mutual recognition under Article 82 of the TFEU. As such, it includes the **direct cooperation of judicial authorities of two Member States** with the possibility to reject an order based only on specific non-recognition grounds as listed in the Directive.[271] There are no special provisions on electronic evidence under the mentioned EIO system. **Only for real time interceptions and cross-border wiretapping do specific rules apply**.[272] This means that for electronic evidence such as subscriber, traffic/transactional and content data, the general system as described further below applies. The EIO will be used in parallel with the new EU e-evidence system. Consequently, the authorities can choose to use either the EIO, the European Production Order, or both.

269 As the focus is on cross-border aspects inside the EU, we did not provide a more detailed analysis of the Second Additional Protocol to the Budapest Convention, neither on other EU instruments outside mutual recognition that have some provisions on the gathering of certain e-evidence, for example the Digital Services Act. See in that regard Eurojust, Digital Services Act and access to information held by service providers, 2024, https://www.eurojust.europa.eu/sites/default/files/assets/digital-services-act-and-access-to-information-held-by-service-providers.pdf.

270 The logic similar to the new EU e-evidence approach is present in the Second Additional Protocol to the Council of Europe Cybercrime Convention.

271 Certain specific aspects, crucial for electronic evidence within the EIO system, will be further evaluated below, considering the extensive material on EIO application. See, for example, Joint Note of Eurojust and the EJN on the practical application of the European Investigation Order, 2019, https://www.eurojust.europa.eu/publication/joint-note-eurojust-and-ejn-practical-application-european-investigation-order; EuroCoord, Best practices for EUROpean COORDination on investigative measures and evidence gathering, 2019, https://www.ejn-crimjust.europa.eu/ejn/libdocumentproperties/EN/3680; Eurojust, Report on Eurojust's casework in the field of the European Investigation Order, November 2020, https://www.eurojust.europa.eu/sites/default/files/2020-11/2020-11_EIO-Casework-Report_CORR_.pdf; EIO-LAPD Project, Guidelines - European Investigation Order, September 2021, https://lapd.pf.um.si/wp-content/uploads/2022/01/Guidelines_EN_final.pdf. See also A. Erbežnik, M. Bonačić: European Investigation Order, E-Evidence and the Future of Cross-Border Cooperation in the EU, in K. Ambos et al., The European Investigation Order Legal Analysis and Practical Dilemmas of International Cooperation, Berlin, 2023, pp. 243–262.

272 EIO Directive, Articles 28, 30, 31.

6.3.1.1. Scope and Types of Proceedings Covered

The scope of the EIO covers **not only criminal proceedings *stricto sensu,*** but also encompasses a wider range of activities. It includes three additional sets of proceedings, namely:

i. proceedings brought by administrative authorities in respect of acts which are punishable under the national law of the issuing State by virtue of being infringements of the rules of law and where the decision may give rise to proceedings before a court having jurisdiction, in particular, in criminal matters;
ii. proceedings brought by judicial authorities in respect of acts which are punishable under the national law of the issuing State by virtue of being infringements of the rules of law, and where the decision may give rise to proceedings before a court having jurisdiction, in particular, in criminal matters;
iii. proceedings in connection with proceedings referred to beforehand, which relate to offences or infringements for which a legal person may be held liable or punished in the issuing State.[273]

The expansion to additional proceedings is not new. It was already present in the Schengen Convention[274] and in the same form in the 2000 EU MLA Convention[275] (which was also mimicked by the Second Additional Protocol to the Council of Europe 1959 MLA Convention[276]), as well as in the EEW.[277] Consequently, the EIO covers procedures regarding a **'criminal charge' in the autonomous meaning of Article 6 of the ECHR and based on the ECtHR Engel criteria**.[278] These criteria include the national classification, the nature of the offence, and the severity of penalty.[279] Such an understanding is also in line with the legal basis of the EIO Directive - Article 82 TFEU. Past cases, like the European Protection Order,[280] clarified that the same instrument should not mix civil and criminal law measures, considering the proposed legal basis. However, **the EIO is not intended (and shall not be misused) for administrative cooperation**, such as cooperation between tax authorities, or for civil confiscations. This delimitation is important, as administrative authorities, such as tax authorities, are increasingly using electronic evidence. In view of defence rights, it is important that the EIO system can be used by both, prosecution and defence.

6.3.1.2. Issuing Authority

The EIO is a judicial decision, whereby the definition of 'judicial authority' is left to the Member States. The Directive itself only refers to the 'issuing authority'. However, in view of the legal basis of Article 82 TFEU, which refers to judicial cooperation in criminal law, **the typical meaning covers prosecutor and judges, investigative judges, and courts as issuing authorities**.[281] Unlike the European Arrest Warrant, the national status of the prosecutor in the issuing States is not important.[282] **As regards other atypical issuing authorities, a validation procedure has been introduced** in cases of '*any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law*'.[283]

273 See also Eurojust report, supra, pp. 15–20, especially in view of cross-border surveillance. For measures not covered see the Joint EJN/Eurojust note, supra, p. 6.

274 Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239, 22.9.2000, p. 19.

275 Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ L C 197, 12.7.2000, p. 1.

276 Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, ETS No 182, Strasbourg, 8.11.2001.

277 Framework Decision 2008/978/JHA on the European Evidence Warrant, OJ L 350, 30.12.2008, p. 72.

278 ECtHR, *Engel and Others v. Netherlands*, a. nos. 5100/71, 5101/71, 5102/71, 5354/72, 5370/72, judgment of 8 June 1976.

279 See Council of Europe, Guide on Article 6 of the Convention – Right to a fair trial (criminal limb), 2014, http://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf.

280 Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European Protection Order, OJ L 338, 21.12.2011, p. 2.

281 EIO Directive, Article 2(c)(i).

282 CJEU, case C-584/19, Staatsanwaltschaft Wien v A. and Others.

283 EIO Directive, Article 2(c)(ii).

Hence, the EIO must be either issued or at least validated by a 'classical' judicial authority (judge, prosecutor) before being sent to the executing Member State. This is especially important given the common encroachment of electronic evidence on the right to privacy, which has emerged as a fundamental right in the technological age.

6.3.1.3. Executing Authority

The executing authority is defined as an 'authority having competence to recognise an EIO and ensure its execution in accordance with the procedures applicable in a similar domestic case'.[284] However, to respect the role of a judge in the executing State for specific measures, it is clearly specified that, **where the procedure in the executing Member State (for example, for specific electronic evidence) requires a court authorisation, 'such an authorisation has to be sought by the executing authorities before executing the request'**. To provide a practical example: a request for IP addresses in issuing Member State A can only be authorised by a prosecutor, who issues an EIO in this regard to be executed in Member State B. However, in Member State B, court authorisation is necessary to execute it. Consequently, police authorities in Member State B must obtain a court authorisation in Member State B before executing the order (as foreseen in a national case for IP addresses). In this regard, the EIO differentiates substantially from the EU e-evidence system, as will be explained further below.

6.3.1.4. Form and Conditions for Issuing

The content and the form of the EIO are explicitly outlined in the Annex to the EIO Directive. However, the most important information to be included in an EIO is already listed in the operative part of the Directive.[285] These include:

- data about the issuing authority (as well as validating authority, if
- applicable);
- the object and reasons for the EIO;
- the necessary information on the person concerned (meaning information to identify the person against which an investigative measure shall be conducted);
- a description of the criminal act and provisions of criminal law (important for the question of double criminality issues if applicable);
- a description of the investigative measure and evidence to be obtained.

The Directive gives Member States the **option to indicate other languages (besides their official language(s))** in which an EIO can be accepted. Based on this, the competent authority of the issuing State must translate the EIO into an official language of the executing State or any other language indicated by the executing State as specified previously.[286]

284 EIO Directive, Article 2(d).

285 EIO Directive, Article 5.

286 See the Eurojust report, supra, p. 13, on the practical and more flexible application, especially in urgent cases.

The issuing authority may only issue an EIO where the following conditions have been met:

a. the issuing of the EIO **is necessary and proportionate** for the purpose of the proceedings, considering the rights of the suspected or accused person; and
b. the investigative measure(s) indicated in the EIO **could have been ordered under the same conditions in a similar domestic case**.

Hence, the EIO Directive specifically addresses the issue of a proportionality test that must be conducted by the issuing authority. There is no proportionality test foreseen in the executing State. The later can only consult the issuing State in that regard. However, the decision remains with the issuing State. Nevertheless, an obvious disproportionate request could amount to ground for non-recognition based on fundamental rights (see further below).[287] A further ground for non-recognition in Article 11 reflects proportionality, namely Article 11(1)(h) – restriction of a measure to certain catalogue offences in the executing State (which does not apply to measures listed in Article 10(2). In addition to this, proportionality is also addressed in Article 10(3), which recommends recourse to another less intrusive measure that achieves the same result. Even more important is the prohibition of forum shopping in Article 6(1)(b) of the EIO Directive. The instrument cannot be used if the investigative measure(s) indicated in the EIO could not have been ordered under the same conditions in a similar domestic case. Using such measure despite this prohibition would go against the spirit of the Directive – you can only request information that would be permitted in the issuing State.

Therefore, it is specifically **recommended, where e-evidence is concerned, to check whether a national prohibition on data retention**[288] or bulk collection of data applies in the issuing State.[289] The completed EIO must be transmitted by any means capable of producing a written record under conditions allowing the executing State to establish authenticity.[290] However, this should be done in a digitalised form through a decentralised IT system, of which the e-Codex system is the backbone.[291]

6.3.1.5. Coercive Measures and Availability of Measures in the Executing State

An executing State can only execute measures that exist under its own national system and are regulated in its own procedural law. It does not need to introduce or invent measures in response to the request of an issuing State. However, the directive stipulates that **certain measures are always considered to be available under the national system of each Member State**. These measures include the following:

a. the obtaining of **information or evidence which is already in the possession of the executing authority** and the information or evidence could have been obtained, in accordance with the law of the executing State, in the framework of criminal proceedings or for the purposes of the EIO;

287 For example, requesting traffic data for a non-serious offence, like a single bicycle theft, could be considered disproportionate.

288 For the different systems on data retention in the EU after the Digital Rights judgment, see https://fra.europa.eu/en/publication/2017/data-retention-across-eu. See also Birrer A., et al.: The state is watching you—A cross-national comparison of data retention in Europe, Telecommunications Policy, Vol. 47, No 4, May 2023.

289 To avoid problems as seen in the EncroChat or SkyECC cases, see CJEU, case C-670/22.

290 EIO Directive, Article 7(1)

291 See Regulation (EU) 2023/2844 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation, and Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), OJ L 150, 1.6.2022, p. 1. See also the Evidence2e-Codex project, supra.

b. the obtaining of **information contained in databases held by police or judicial authorities** and directly accessible by the executing authority in the framework of criminal proceedings;
c. the **hearing of a witness, expert, victim, suspected or accused person or third party** in the territory of the executing State;
d. any **non-coercive investigative measure as defined under the law of the executing State**;
e. the **identification of persons holding a subscription** of a specified phone number or **IP address**.

In view of electronic evidence, subscriber data and IP addresses are considered as always available (see point (e) above). With regards to other electronic evidence, such as traffic/transactional data, the issue of existing evidence and the application of non-coercive measures can arise. The term **'coercive' (see point (d) above) is defined in a broad sense to mean all measures that infringe upon personal liberties in an invasive manner**. This includes invasive measures into the right to privacy.[292] Certain investigative techniques such as bulk collection of electronic evidence, for example, are not considered coercive in the classical sense, as no physical coercion or force is used. However, they are extremely invasive in terms of the right to privacy and, as such, should not be considered as non-coercive. **This distinction between available and not-available measures under the EIO Directive is crucial in view of the grounds of non-recognition**. For the measures that are always available, two grounds for non-recognition cannot be used, namely dual criminality outside the list of the 32 offences, and catalogue offences. The rest of the non-recognition grounds do apply. If the requested measure does not exist under the law of the executing State, or it would not be available in a similar domestic case, and there is no other investigative measure that would achieve the same result, then the EIO is not recognised, and the issuing authority must be informed about it.

6.3.1.6. Assessment in the Executing State and Non-Recognition Grounds

The Directive continues the trend of adhering to the ***forum regit actum*** **principle** (the rules of the issuing State) as closely as possible. This trend began with the 2000 EU MLA Convention,[293] and was further reflected in the Second Additional Protocol to the 1959 Council of Europe Convention[294]. To prevent potential issues with the admissibility of evidence in the issuing State, the *forum regit actum* principle should be used if it is 'not contrary to the fundamental principles of the law of the executing State'. The recognition of the EIO is based on the principle of mutual recognition as defined in Article 82 TFEU. **Consequently, an EIO must be automatically recognised, and the executing authority has only a limited ability to assess the request within the framework of one of the explicit non-recognition grounds**. Most of these grounds are listed in Article 11, with additional ones in other parts of the text, such as Article 9(3), which clarifies that the EIO has to be issued or validated by a judicial authority. If this is not the case, it must be returned, meaning it is not recognised by the executing State. If an EIO is denied, the issuing Member State may have the appropriate authority reissue a new EIO.

292 This was clarified in Recital 16 of the EIO Directive: 'Non-coercive measures could be, for example, such measures that do not infringe the right to privacy or the right to property, depending on national law.' See also EuroCoord, supra, pp. 20–28.

293 See the EU MLA Convention, supra, Article 3.

294 See the CoE MLA Convention as modified by the 2nd Additional Protocol, supra, Article 1.

The non-recognition grounds listed in Article 11(1), points (a) to (h), of the EIO Directive can be divided into three categories as regards their intention:

i. **those in the interest of the State**: points (b), (c) and (e);
ii. **those in the interest of the suspect**: points (a), (d), and (f);
iii. **those that serve both interests**: points (e), (g) and (h).

(I) IN THE INTEREST OF THE STATE

(b) in a specific case the execution of the EIO would harm essential national security interests, jeopardise the source of the information or involve the use of classified information relating to specific intelligence activities;

(c) the EIO has been issued in proceedings referred to in Article 4(b) and (c) and the investigative measure would not be authorised under the law of the executing State in a similar domestic case;

(e) the EIO relates to a criminal offence which is alleged to have been committed outside.

(II) IN THE INTEREST OF THE SUSPECT

(a) there is an immunity or a privilege under the law of the executing State which makes it impossible to execute the EIO or there are rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media, which make it impossible to execute the EIO;295

(d) the execution of the EIO would be contrary to the principle of ne bis in idem;[296]

(f) there are substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the Charter.[297]

(III) BOTH INTERESTS

(e) the EIO relates to a criminal offence which is alleged to have been committed outside the territory of the issuing State and wholly or partially on the territory of the executing State, and the conduct in connection with which the EIO is issued is not an offence in the executing State;

(g) the conduct for which the EIO has been issued does not constitute an offence under the law of the executing State, unless it concerns an offence listed within the categories of offences set out in Annex D of the EIO Directive, as indicated by the issuing authority in the EIO, if it is punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least 3 years;[298] or

(h) the use of the investigative measure indicated in the EIO is restricted under the law of the executing State to a list or category of offences or to offences punishable by a certain threshold, which does not include the offence covered by the EIO.

Table 4: Non-recognition grounds (EIO)

295 Such privilege could be political immunity or professional privilege like a lawyer's or doctor's privilege.

296 The ne bis in idem principle has been introduced in a more open way following the Charter than the past interpretation of the Court of Justice EU as regards EAW procedures based on Article 54 CISA (Convention on Implementation of the Schengen Agreement) demanding also an execution of the sentence. Extensive case-law of the CJEU on ne bis in idem must be taken into account – see, for example, CJEU, van Esbroeck, C-436/04, Kraaijenbrink, C-367/05, Mantello, C-261/09, Spasic, C-129/14 PPU, Åkerberg Fransson, C-617/1027 May 2014, Kossowski, C-486/14, etc. See, also, Eurojust, Case-law by the Court of Justice of the European Union on the European Arrest Warrant, 2023, pp. 93-101, as the same interpretation of ne bis in idem as for the EAW applies also for the EIO system.

297 Article 6 of the TEU refers to three levels of fundamental rights, namely ECHR minimum, the EU Charter and common constitutional traditions. Consequently, any of this could be used as a non-recognition ground in the framework of the EIO.

298 This is the classical list of 32 offences punishable above 3 years as already introduced by the EAW.

While most non-recognition grounds are concentrated in Article 11, they are not exclusive to it. **Additional non-recognition grounds** include:

- the non-issuance or non-validation by a judge or prosecutor (Article 9(3));
- the non-existence and non-availability of a measure (Article 10(5)); and
- specific grounds for certain measures regulated in detail in the special
- part, for example the *ordre public* ground for such measures.[299]

Specific rules apply to electronic evidence for subscriber data and IP addresses. According to Article 10, such electronic evidence is considered always available. Consequently, two grounds for non-recognition, namely points (g) and (h), do not apply. This implies that such data can be requested even if the offence is not considered criminal in the executing State, and the executing State cannot impose limitations based on a catalogue of offences or a threshold. However, this does not apply for traffic/transactional and content data.

6.3.1.7. Deadlines

The EIO Directive provides **maximum deadlines** for the recognition and execution of the requested investigated measure. Specifically, the decision to recognise the Order should be taken in **30 days**, with the possibility of an extension for an **additional 30 days** in duly justified cases. Once recognised, the measure must be **executed in 90 days**. However, it is important to note that these time limits represent the maximum allowable duration. As previously mentioned, the Directive **strongly encourages the application of the *forum regit actum*** principle. Consequently, when the issuing authority specifies in the EIO that, due to procedural deadlines, the seriousness of the offence, or other particularly urgent circumstances, a shorter deadline than those provided in this Article is necessary, or if the issuing authority designates a specific date for the investigative measure's execution, the executing authority should consider these requirements. In cases where it is not practicable for the competent executing authority to meet the mentioned time limits, the executing authority is obliged to inform the issuing authority about the reasons for the delay and the estimated time necessary for providing a decision or execution.[300]

However, a specific deadline applies to provisional measures preventing the destruction, transformation, removal, transfer or disposal of an item that may be used as evidence. The executing authority shall decide and communicate the decision on the provisional measure as soon as possible and, wherever practicable, within 24 hours of receipt of the EIO. For its implementation, the normal deadlines still apply. After consulting the issuing authority, the executing authority may, in accordance with its national law and practice, lay down appropriate conditions considering the circumstances of the case to limit the period for which the provisional measure is to be maintained. If, in accordance with those conditions, it envisages lifting the provisional measure, the executing authority must inform the issuing authority, which shall be given the opportunity to submit its comments. The issuing authority shall forthwith notify the executing authority that the provisional measure referred has been lifted.[301]

299 See EIO Directive, Articles 22–31.

300 EIO Directive, Article 12. The mentioned deadlines were presented as one of the arguments for the new e-evidence system.

301 EIO Directive, Article 32.

6.3.1.8. Legal remedies

Legal remedies available to individuals affected by the EIO (not necessarily the suspect), must be **equivalent to those available in a similar domestic case**.[302] This means either providing the same remedies or achieving an equivalent result. However, if there are no specific legal remedies available for a particular measure at national level, there is no obligation to introduce such remedies for EIO measures. In such cases, the time limits for seeking a legal remedy should be the same as those provided in a similar national case to ensure an effective exercise of rights. **The EIO system is based on effective legal remedies in the issuing State. The absence of such remedies in the issuing State may prohibit to use the EIO system, according to CJEU case-law**. In the case C-852/19, *Gavanozov II*, the court ruled that legislation from a Member State issuing a European Investigation Order, which does not provide any legal remedy against measures such as searches, seizures, or witness hearings conducted by videoconference, is precluded.

Due to mutual recognition, **substantive reasons for issuing the EIO can only be challenged in the issuing State**.[303] Any alternative approach would contradict the principle of mutual recognition and impose a content-based assessment on the executing State. However, the lack of evaluation of substantive reasons in the executing State cannot be to the detriment to the **executing State's obligations concerning fundamental rights' protection** ('without prejudice to the guarantees of fundamental rights in the executing State'). However, a defendant must establish *prima facie* evidence of a real risk of a violation of their fundamental rights. When there are no confidentiality concerns, the person affected should be informed about the possibility of seeking legal remedies, and these remedies must be effective. Both the issuing and executing authorities have an obligation to inform each other regarding the legal remedies used during the issuing, recognition, and execution of the EIO. It is important to note that **the Directive does not govern the admissibility of evidence**, which remains a national prerogative. Nevertheless, like in the Directive on access to a lawyer[304], the EIO Directive contains **a general reference to ensure that 'rights of the defence and the fairness of the proceedings are respected when assessing evidence obtained through the EIO'** (subject to national procedural rules). This reference implies adherence to minimum standards outlined in the ECHR, particularly concerning Article 8 ECHR concerning e-evidence. It establishes an evolving EU admissibility rule.[305]

CHECKLIST OF EIO KEY POINTS

- ☐ Ensure that the procedures using an EIO pertain to a 'criminal charge'.
- ☐ In case of doubt, apply the Engel criteria, which include a national classification, the nature of the offence, and the sanction involved.
- ☐ Check in advance that your national system offers effective remedies for the requested measure.

302 EIO Directive, Article 14.

303 Such a remedy in the issuing State must be an effective one, including access to evidence from the executing State. See Italian Supreme Court, case No 44154/23, supra.

304 Directive 2013/48/EU on the right of access to a lawyer, supra.

305 It was further developed in Directive (EU) 2016/343 on the presumption of innocence, supra.

- ☐ Verify that the issuing authority is either a prosecutor or a judge. The national status of a prosecutor does not impact this requirement.
- ☐ If the issuing authority is a police/administrative body, ensure that the Order has been validated by a national prosecutor or judge before dispatch.
- ☐ Ensure that the executing authority is the same as the authority responsible for such measure in the national system.
- ☐ If a court order is required for the requested measure in your national system, ensure to request one.
- ☐ Use the EIO form in the directive annex to transfer the request. Fill in the form as thoroughly as possible, providing as much information as possible regarding the offence, including a short description of the factual basis.
- ☐ Check what languages the executing Member State accepts.
- ☐ Check for any possible differences in the measure and admissibility rules between the issuing and executing State beforehand.
- ☐ Check beforehand whether the requested measure is available in the executing State.
- ☐ Ensure that your request does not amount to forum shopping – that is, requesting something that is not permitted under your national system to circumvent national safeguards.
- ☐ Remember that the assessment in the executing State is not a new full-content assessment. It is limited to non-recognition grounds within the provided deadlines.
- ☐ If something is unclear, please contact the executing authority.
- ☐ For subscriber data, IP addresses, and other non-coercive electronic data, dual criminality and catalogue offences limitations do not apply.
- ☐ Before sending the request, please verify the deadlines in the executing State. If your national deadlines or procedural requirements differ from those of the executing State, you should request that the executing State considers them (by indicating them in the Order).
- ☐ The executing State should consider your request unless it contradicts fundamental principles of their national law.
- ☐ It is important to note that the deadlines specified in the Directive represent maximum time limits.
- ☐ Maintain communication with the other State to inform them about the legal remedies employed by the affected person in your country.
- ☐ In the executing State, legal remedies should be restricted to the procedural aspects of the measure within its territory, as well as issues related to fundamental rights.

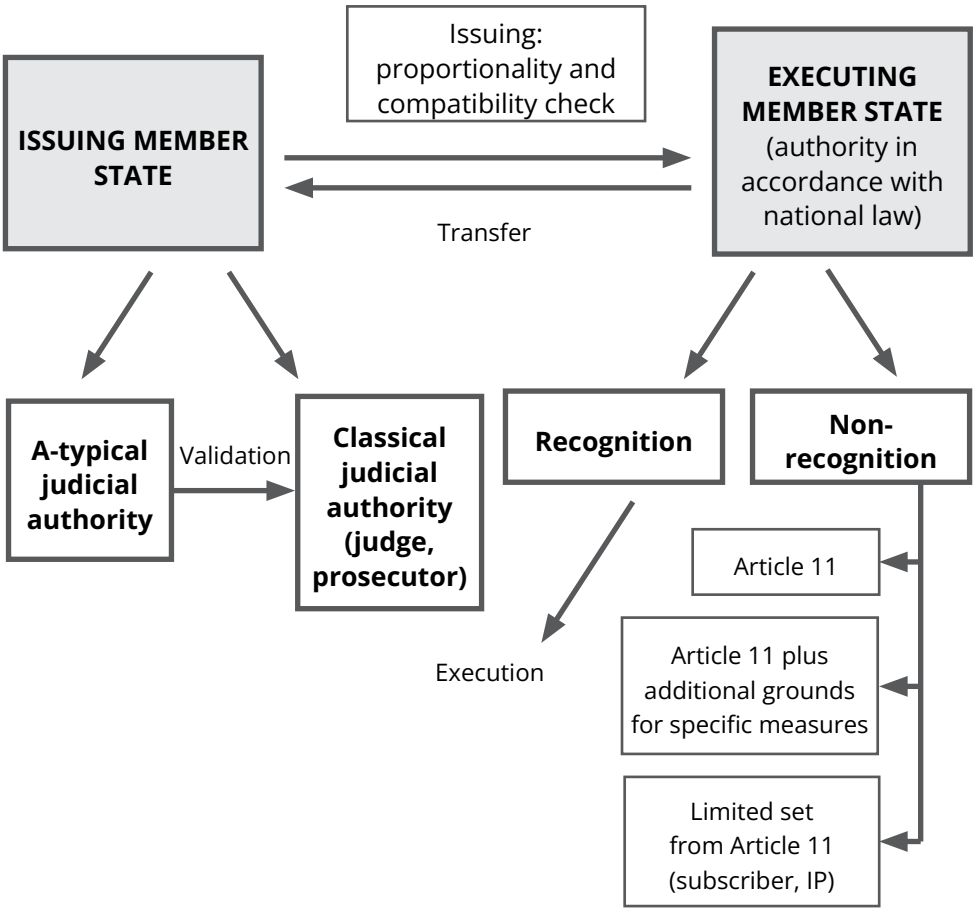

Figure 9: EIO system

6.3.2. EU e-Evidence System – Regulation (EU) 2023/1543 and Directive (EU) 2023/1544[306]

This Section concerns two legislative instruments which were introduced in Section 3 of this Toolkit, **namely Regulation (EU) 2023/1543 on the European Production and Preservation Orders for electronic evidence in criminal matters** (based on Article 82 of the TFEU), and **Directive (EU) 2023/1544 laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings** (based on Articles 53 and 62 of the TFEU). The main feature of the new system is the **direct issuance of Preservation and Production Orders from one Member States to a telecommunication provider in another**, without the participation of authorities from the second Member State in principle. The second State involves itself only in the case of certain categories of data, provided the case is not considered 'domestic' and there are problems with enforcement. This is reflected in the terminology, as the term 'enforcing State' is used instead of 'executing State'. The system also introduces the presumption that third country providers offering services in the EU are considered as EU providers. However, there is a difference in application between the two proposals that form e-evidence. While the directive binds all Member States, this does not apply to the Regulation. The new system will be explained in further detail below.[307]

306 This Section is a summary from A. Erbežnik, International Encyclopaedia of Laws, EU Criminal Law, Kluwer, 2024. See also A. Erbežnik: Uvod v kazensko procesno pravo RS in EU, GV Založba, 2022, pp. 442–448.

307 See also M. Bonačić: Pristup elektroničkim dokazima: na putu prema novom modelu kaznenopravne suradnje u EU, Hrvatska akademija znanosti i umjetnosti, 2022, pp. 71–97; T. Christakis: E-Evidence in the EU Parliament: Basic Features of Birgit Sippel's Draft Report, European Law Blog, 2020; A. Tinoco-Pastrana: The Proposal on Electronic Evidence in the European Union, eucrim, No 1/2020, pp. 46-50; S. Tosza: The European Commission's Proposal on Cross-Border Access to E-Evidence, eucrim, No 4/2018, pp. 212–219; S. Tosza: All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order, New Journal of European Criminal Law, Vol. 11, No 2/2020, pp. 161–183; A. Erbežnik: A new EU system on cross-border gathering of e-evidence – analysis and open questions, Dignitas, No 98/2023, pp. 47–72.

6.3.3. Scope and Types of Proceedings Covered

The system is intended solely for use in *criminal proceedings stricto sensu*, not for other types of proceedings in criminal matters (as was the case for the EIO). It also applies to **legal persons**, regardless of the different national systems concerning the criminalisation of legal persons. The system is limited to **historical telecommunication data** and does not include real time interceptions. For real-time interceptions, the EIO must be applied. However, during legislative negotiations, the system's scope was broadened to include **searches for absconding persons**, provided the decision was not rendered *in absentia* and the detention Order is for at least 4 months. It is expressly prohibited to 'cluster' proceedings in a manner that would allow the order to be used for mutual legal assistance requests from other States.[308] It can also be used by the defence within the framework of applicable defence rights in accordance with national criminal procedural law.[309]

6.3.3.1. Types of e-Evidence Covered

In terms of telecommunication services, the services covered include:

a. electronic communications services as defined in Article 2, point (4), of Directive (EU) 2018/1972 establishing the European Electronic Communications Code;[310]
b. Internet domain name and IP numbering services, such as IP address assignment, domain name registry, domain name registrar and domain name-related privacy and proxy services;
c. other information society services as referred to in Article 1(1), point (b), of Directive (EU) 2015/1535[311] that enable their users to communicate with one another, or make it possible to store or otherwise process data on behalf of the users to whom the service is provided, provided that the storage of data is a defining component of the service provided to the user.[312]

This could cover subscriber data, IPs, classical e-mails, SMS data, metadata, and communications via applications like Viber, WhatsApp, or Signal, as well as gaming platform chats, etc. The categories of telecommunication data covered include subscriber data, traffic data, and content data, with only historical telecommunication data being covered.[313] The original proposal from the Commission also introduced a new category termed 'access data', positioned between subscriber and traffic data, primarily concerning IP addresses and certain other identifiers. However, this category was not included in the final text to maintain clear distinctions between the classical categories of telecommunication data. Instead, the final text assigns a special role to 'data requested solely for the purpose of identifying the user', primarily involving IP addresses, source ports, and timestamp data. The definitions of the different data categories are the following:

308 Regulation (EU) 2023/1543, Article 2.

309 EIO Directive, Article 1(2).

310 OJ L 321, 17.12.2018, p. 36.

311 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241, 17.9.2015, p. 1.

312 Regulation (EU) 2023/1543, Recital 27 and Article 3, point 3.

313 Regulation (EU) 2023/1543, Article 3, point 8.

Data category	Description
(1) 'subscriber data'	Any data held by a service provider relating to the subscription to its services, pertaining to: the identity of a subscriber or customer, such as the provided name, date of birth, postal or geographic address, billing and payment data, telephone number, or e-mail address; the type of service and its duration, including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer at the moment of initial registration or activation, and data related to the validation of the use of the service, excluding passwords or other authentication means used instead of a password that are provided by a user, or created at the request of a user.[314]
(2) 'data requested for the sole purpose of identifying the user'	IP addresses and, where necessary, the relevant source ports and time stamp, namely the date and time, or technical equivalents of those identifiers and related information, where requested by law enforcement authorities or by judicial authorities for the sole purpose of identifying the user in a specific criminal investigation.[315]
(3) 'traffic data'	Data related to the provision of a service offered by a service provider which serve to provide context or additional information about such service and are generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression, and other electronic communications metadata and data, other than subscriber data, relating to the commencement and termination of a user access session to a service, such as the date and time of use, the log-in to and log-off from the service.[316]
(4) 'content data'	Any data in a digital format, such as text, voice, videos, images and sound, other than subscriber data or traffic data.[317]

Table 5: Definitions of the data categories (EPO)

314 Regulation (EU) 2023/1543, Article 3, point 9.

315 Regulation (EU) 2023/1543, Article 3, point 10.

316 Regulation (EU) 2023/1543, Article 3, point 11.

317 Regulation (EU) 2023/1543, Article 3, point 12.

6.3.3.2. Domestic v. Non-Domestic Case

Traffic and content data are further categorised based on whether they pertain to a 'domestic' or 'non-domestic' case.[318] A **'domestic' case** is identified by the issuing authority based on reasonable grounds to believe that:

- the offence has been committed, is being committed or is likely to be committed in the issuing State;
- **and the person whose data are requested resides in the issuing State**.[319]

These criteria are deliberately broad, with further details provided in the recitals. The first criterion considers the offence's location as per the laws of the issuing State,[320] acknowledging that national criminal codes may apply extraterritorially, such as under the universality principle. The **concept of 'residence'**- the second criterion - is determined not necessarily by official residence permits but through a factual, objective assessment on a case-by-case basis by the issuing State. **This assessment considers whether an individual has made a particular Member State their habitual centre of interests or intends to do so**. Indicators of reasonable grounds for residence include possession of an identity card or residence permit, intentions to settle, stable presence, family or economic ties, a registered vehicle, or a bank account. However, mere short visits or holiday stays without significant links do not constitute residence. This differentiation between data categories and the classification of cases as 'domestic' or 'non-domestic' is crucial for the roles of issuing and executing/enforcing authorities.

6.3.3.3. Issuing Authority

The issuing authority for **subscriber data and 'data requested for the sole purpose of identifying the person'** must be a **prosecutor or judge**. In the case of **traffic and content data**, the issuing authority must be a **judge**.[321] Should the issuing authority not be a prosecutor or judge, as required by the category of data, a validation procedure similar to that of the European Investigation Order (EIO) has to take place. This means that if national law of the issuing state permits a police authority to request subscriber data or IP addresses, such an order must undergo validation by a prosecutor or judge before being sent. Central authorities, tasked solely with administrative duties related to the transmission or receipt of orders, certificates, and notifications, may assist these authorities. The Regulation also outlines specific provisions and procedures for **'emergency cases'**. In such a case, as defined by the Regulation, a European Production Order for subscriber data, or data requested for the sole purpose of identifying the user, or a European Preservation Order can be issued exceptionally without prior validation. This exception permissible only when validation cannot be timely secured, and the authorities would have the capacity to issue such an Order in a similar domestic case without such validation. The issuing authority is then obliged to obtain *ex-post* validation of the order without undue delay, and at the latest within 48 hours after issuance. If this *ex-post* validation is not granted, the issuing authority is compelled to immediately withdraw the Order or otherwise restrict the use of any data obtained.

318 Such a definition is not used in the articles but in the recitals.

319 Regulation (EU) 2023/1543, Article 8(2).

320 For instance, jurisdiction can be based both on where the perpetrator acted and where the prohibited consequence occurred, provided that the national law of the issuing State allows for such criteria.

321 CJEU case-law on data retention triggered a harmonisation of authorities being able to order access to traffic data - see case CJEU, Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net et al.

6.3.3.4. Enforcing Authority

The **'enforcing authority'** refers to the authority in the enforcing State which, according with the national law of that State, is competent to receive a European Production Order or a European Preservation Order transmitted by the issuing authority for the purpose of notification or enforcement.[322] This system promotes the principle of mutual recognition and accordingly limits the role of the authority in the recipient State, a concept that is reflected in the choice of terminology. The term 'enforcing authority' is preferred over 'executing authority' to emphasise its streamlined role. However, it is essential that the enforcing authority **is of a comparable nature to that which would handle a similar national measure, to prevent any internal constitutional issues**.[323] Certain legal issues may arise in cases where the issuing State does not require court authorisation (for example, for IP addresses) but the enforcing State does.[324]

6.3.3.5. Conditions for Issuing

– **GENERAL CONDITIONS**

The same two main conditions apply as in the case of issuing a European Investigation Order (EIO), namely:

a. **proportionality**, which also considers the rights of the suspect; and
b. **prohibition of forum shopping**, where the Order could have been issued under the same conditions in a similar domestic case.[325]

In addition, certain specific conditions apply regarding nature of criminal offences, and privileges and immunities. The same criteria apply also to a Preservation Order, which must be necessary and proportionate for the purpose of preventing the removal, deletion, or alteration of data.[326]

– **CRIMINAL OFFENCES**

A Production Order for **subscriber data and data requested for the sole purpose of identifying the user, or a Preservation Order**, may be issued for **all criminal offences**.

However, a Production Order **for traffic and content data** may only be issued for the following offences:

a. criminal offences punishable in the issuing State by a custodial sentence of a **maximum of at least 3 years**; or
b. offences that are wholly or partly committed **by means of an information system and referring to combating fraud and counterfeiting of non-cash means of payment,**[327] **combating the sexual abuse and sexual exploitation of children and child pornography,**[328]**and on attacks against information systems**;[329] or
c. criminal offences as defined in Articles 3 to 12 and 14 of Directive (EU) 2017/541 on **combatting terrorism**;[330] or
d. for the **execution of a custodial sentence or a detention order of at least 4 months**, following criminal proceedings, imposed by a decision

322 Regulation (EU) 2023/1543, Article 3, point 17.

323 See Recital 61 stating that '[w]here a notification to the enforcing authority, or enforcement, takes place in accordance with this Regulation, the enforcing State could provide under its national law that the execution of a European Production Order might require the procedural involvement of a court in the enforcing State'.

324 See, for example, the Cybercrime Convention Committee, Conditions for obtaining subscriber information in relation to dynamic versus static IP ad- dresses: overview of relevant court decisions and developments, T-CY(2018)26, https://rm.coe.int/t-cy-2018-26-ip-addresses-v6/16808ea472. See also ECtHR, *Benedik v. Slovenia*, a. No 62357/14, judgment of 24 April 2018.

325 Regulation (EU) 2023/1543, Article 5.

326 Regulation (EU) 2023/1543, Article 6. A Preservation Order is in anticipation of a subsequent request for the production of those data, whether through mutual legal assistance, a European Investigation Order (EIO), or a European Production Order.

327 OJ L 123, 10.5.2019, p. 18.

328 Articles 3 to 7 of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, OJ L 335, 17.12.2011, p. 1.

329 Articles 3 to 8 of Directive 2013/40/EU on attacks against information systems, OJ L 218, 14.8.2013, p. 8

330 OJ L 88, 31.3.2017, p. 6.

that was not rendered in absentia, in cases **where the person convicted absconded from justice**, for criminal offences referred to in points (a), (b) and (c).[331]

– **PRIVILEGES AND IMMUNITIES**

If the issuing authority has reasons to believe that the traffic data, except for data requested for the sole purpose of identifying the user, or the content data requested by the European Production Order are protected by immunities or privileges granted under the law of the enforcing State, or that those data are subject in that Member State to rules on determination and limitation of criminal liability relating to freedom of the press or freedom of expression in other media, the issuing authority may seek clarification before issuing the Order. The **issuing authority shall not issue a European Production Order if it finds that the requested traffic data, except for data requested for the sole purpose of identifying the user, or the content data are protected by immunities or privileges granted under the law of the enforcing State**, or that those data are subject in that Member State to rules on determination and limitation of criminal liability relating to freedom of the press and freedom of expression in other media.[332]

– **INFORMATION OF THE ORDER AND TRANSMISSION**

The Order should include the following information:

a. the issuing authority and, where applicable, the validating authority;
b. the addressee of the European Production Order as referred to in Article 7;
c. the user, except where the sole purpose of the Order is to identify the user, or any other unique identifier such as username, login ID or account name to determine the data that are being requested;
d. the requested data category as defined in Article 3, points (9) to (12);
e. if applicable, the time range of the data for which production is requested;
f. the applicable provisions of the criminal law of the issuing State;
g. in emergency cases as defined in Article 3, point (18), the duly justified reasons for the emergency;
h. in cases where the European Production Order is directly addressed to the service provider that stores or otherwise processes the data on behalf of the controller, a confirmation that the conditions set out in paragraph 6 of this Article are met;
i. the grounds for determining that the European Production Order fulfils the conditions of necessity and proportionality;
j. a summary description of the case.[333]

The Order is transmitted via a certificate, either an EPOC (European Production Order Certificate) or an EPOC-PR (European Preservation Order Certificate), which templates are annexed to the Regulation. The amount of information provided varies depending on whether the recipient is the service provider or their legal representative, or the enforcing authority. The latter will receive additional information, specifically the details outlined in points (i) and (j) mentioned above. Where needed, the EPOC or the EPOC-PR must be **translated into an official language of the Union accepted by**

331 Regulation (EU) 2023/1543, Article 5(3) and (4).

332 Regulation (EU) 2023/1543, Article 5(10).

333 Regulation (EU) 2023/1543, Article 5(5).

the addressee. Where no language has been specified by the service provider, the EPOC or the EPOC-PR must be translated into **an official language of the Member State where the designated establishment or the legal representative of the service provider is located**. Where a notification to the enforcing authority is required, the EPOC to be transmitted to that authority must be translated into an official language of the enforcing State or into another official language of the Union accepted by that State.[334]

In terms of the transmission of certificates, a **decentralised IT system is foreseen**. During the transitional period, the use of the most appropriate alternative means will also be employed, taking into account the need to ensure a swift, secure and reliable exchange of information.[335] The issuing authority, and not the provider, is responsible for informing without delay the affected person when data has been requested through a European Production Order, with the possibility to delay such information.[336]

6.3.3.6. Addresses

The recipients of Orders under the e-evidence system are either the **'designated establishment'** or a **'legal representative'** of the concerned service provider.[337] Given the extraterritorial scope of the e-evidence system, it also applies to third-country service providers that offer services within the Union but lack an establishment there. To accommodate these providers, the concept of a 'legal representative' has been introduced, operating under the legal fiction that the representative acts on behalf of the provider. Exceptionally, in emergency situations where the designated establishment or the legal representative of a service provider fails to respond to an Order within the prescribed deadlines, the Order may then be directed to any other establishment or legal representative of the service provider within the Union.[338] Furthermore, when **notification is required** (as detailed below), the certificate is also sent to the **enforcing authority**.[339]

In principle, the provider to be addressed is the one acting as the data controller. However, **in emergency situations, a data processor may also be addressed** under the following conditions: the controller cannot be identified despite reasonable efforts from the issuing authority; or addressing the controller might be detrimental to the investigation (the controller is the suspect itself). In such a case, the issuing authority should also indicate whether the provider must refrain from informing the controller, for as long as necessary and proportionate, in order not to obstruct the relevant criminal proceedings, and provide a short justification. If the data refers to a public authority, it can be only requested where the public authority for which the data are stored or otherwise processed is in the issuing State. Furthermore, if the data refers to a privileged professional in their business capacity under the law of the issuing State (for example, a doctor), traffic and content data may only be requested:

- where the privileged professional resides in the issuing State;
- where addressing the privileged professional might be detrimental to the investigation; or
- where the privileges were waived in accordance with the applicable law.

In principle, the addressee must comply with the Order within the prescribed deadlines and is not entitled to independently assess the validity of the Order.

334 Regulation (EU) 2023/1543, Article 9.

335 Regulation (EU) 2023/1543, Articles 19-26.

336 Regulation (EU) 2023/1543, Article 13.

337 See their definitions in Article 3, points 6 and 7, of Regulation (EU) 2023/1543, and Article 2, points 5 and 6, of Directive (EU) 2023/1544.

338 Regulation (EU) 2023/1543, Article 7.

339 Regulation (EU) 2023/1543, Article 8(1).

Despite this, the addressee has the following possibilities when executing an Order (by using Annex III of the e-Evidence Regulation):

- to inform the issuing authority and the enforcing authority that **the execution of the certificate could interfere with immunities or privileges**, or with rules on the determination or limitation of criminal liability that relate to **freedom of the press or freedom of expression** in other media, under the law of the enforcing State, based solely on the information contained in the certificate;
- without undue delay, inform the issuing authority and, where a notification to the enforcing authority took place pursuant to Article 8, the enforcing authority referred to in the certificate, that the addressee cannot comply with its obligation to produce the requested data because **the certificate is incomplete, contains manifest errors or does not contain sufficient information** to execute it;
- without undue delay, inform the issuing authority and, where a notification to the enforcing authority took place pursuant to Article 8, the enforcing authority referred to in the certificate, that it cannot comply with its obligation to produce the requested data because of a ***de facto* impossibility** due to circumstances not attributable to the addressee, explaining the reasons for such a *de facto* impossibility;
- In all cases where the addressee does not provide the requested data, does not provide the requested data exhaustively or does not provide the requested data within the specified deadline, inform the issuing authority and, where a notification to the enforcing authority took place pursuant to Article 8, the enforcing authority referred to in the certificate, of those reasons.[340]

The recipients of Orders under the e-evidence system are either the 'designated establishment' or a 'legal representative' of the concerned service provider.[341] Given the extraterritorial scope of the e-evidence system, it also applies to third-country service providers that offer services within the Union but lack an establishment there. To accommodate these providers, the concept of a 'legal representative' has been introduced, operating under the legal fiction that this representative act on behalf of the provider. Exceptionally, in emergency situations where the designated establishment or the legal representative of a service provider fails to respond to an Order within the prescribed deadlines, the Order may then be directed to any other establishment or legal representative of the service provider within the Union.[342] Furthermore, when notification is required (as detailed below), the certificate is also sent to the enforcing authority.[343]

In principle, the provider to be addressed is the one acting as the data controller. However, in emergency situations, a data processor may also be addressed under the following conditions: the controller cannot be identified despite reasonable efforts from the issuing authority; or addressing the controller might be detrimental to the investigation (the controller is the suspect itself). In such a case the issuing authority should also indicate if the provider must refrain from informing the controller, for as long as necessary and proportionate, in order not to obstruct the relevant criminal proceedings, and provide a short justification. If the data refers to a public authority, it can be only requested where the public authority for which the data are stored or otherwise processed is in the issuing State. Furthermore, if the data refers to a privileged professional in their business capacity under the law of the issuing State (for example, a doctor), traffic and content data may only be requested:

340 Regulation (EU) 2023/1543, Articles 10, 11.

341 See their definitions in Article 3, points 6 and 7, of Regulation (EU) 2023/1543, and Article 2, points 5 and 6, of Directive (EU) 2023/1544.

342 Regulation (EU) 2023/1543, Article 7.

343 Regulation (EU) 2023/1543, Article 8(1).

- where the privileged professional resides in the issuing State;
- where addressing the privileged professional might be detrimental to the investigation; or
- where the privileges were waived in accordance with the applicable law.

In principle, the addressee must comply with the Order within the prescribed deadlines and is not entitled to independently assess the validity of the Order. Despite this, the addressee has the following possibilities when executing an Order (by using Annex III of the e-Evidence Regulation):

- to inform the issuing authority and the enforcing authority hat the execution of the certificate could interfere with immunities or privileges, or with rules on the determination or limitation of criminal liability that relate to freedom of the press or freedom of expression in other media, under the law of the enforcing State, based solely on the information contained in the certificate;
- without undue delay, inform the issuing authority and, where a notification to the enforcing authority took place pursuant to Article 8, the enforcing authority referred to in the certificate, that the addressee cannot comply with its obligation to produce the requested data because the certificate is incomplete, contains manifest errors or does not contain sufficient information to execute it;
- without undue delay, inform the issuing authority and, where a notification to the enforcing authority took place pursuant to Article 8, the enforcing authority referred to in the certificate, that it cannot comply with its obligation to produce the requested data because of a *de facto* impossibility due to circumstances not attributable to the addressee, explaining the reasons for such a *de facto* impossibility;
- In all cases where the addressee does not provide the requested data, does not provide the requested data exhaustively or does not provide the requested data within the specified deadline, inform the issuing authority and, where a notification to the enforcing authority took place pursuant to Article 8, the enforcing authority referred to in the certificate, of those reasons.[344]

6.3.3.7. Different Types of Procedures

Depending on the type of data, the classification of data as 'domestic' and 'non-domestic' data, as well as the use classification of 'normal' or 'emergency case', the following different options exist:

1. Regular case in obtaining subscriber data and data requested for the sole reason to identify the person.
2. Regular case in obtaining traffic and content data in a 'domestic case'.
3. Regular case in obtaining traffic and content data in a 'non-domestic case'.
4. Emergency cases.

344 Regulation (EU) 2023/1543, Articles 10, 11.

– **OBTAINING SUBSCRIBER DATA AND DATA REQUESTED FOR THE SOLE REASON TO IDENTIFY THE PERSON, AND PRESERVATION OF ALL DATA**

For such data, transmission occurs **directly between the provider** (or its legal representative) **and the issuing authority**, without the involvement or notification of the enforcing authority. The data must be transferred from the provider to the issuing authority within the specified deadline, which is set at **10 days** for normal cases and 8 hours for urgent cases. **The enforcing authority only becomes involved if the provider fails to fulfil its obligation**.[345]

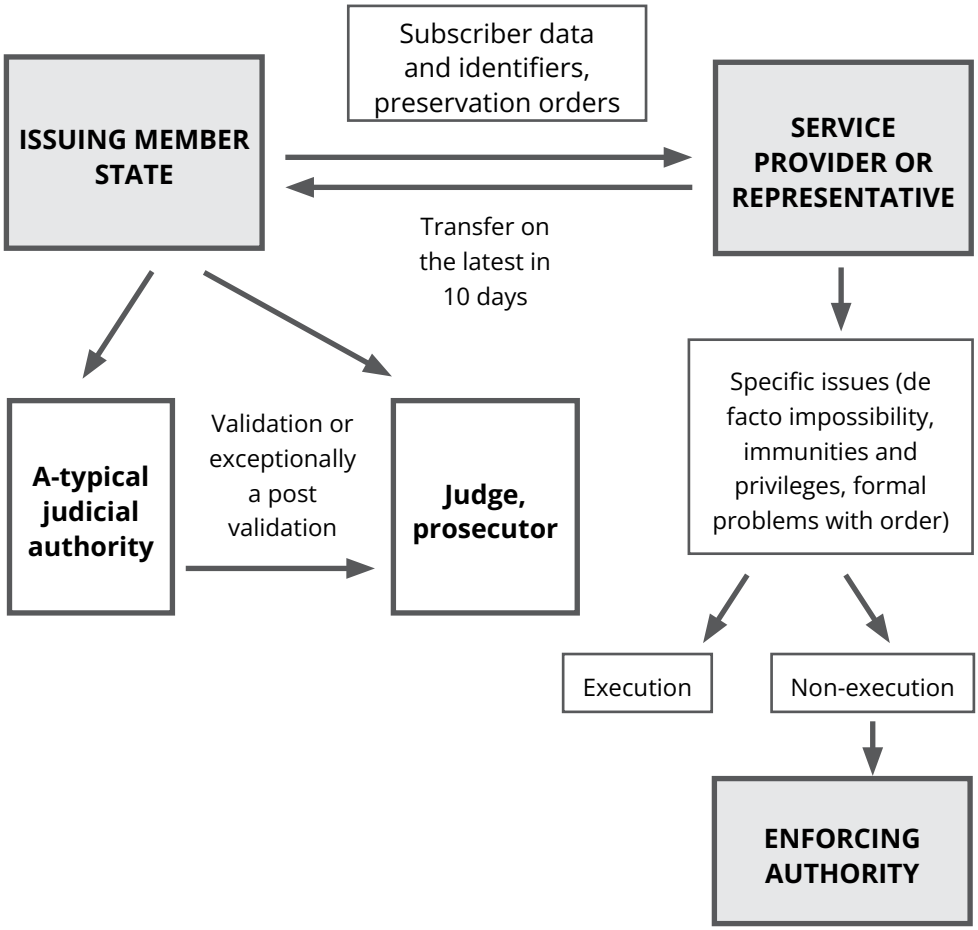

Figure 10: Regular case in obtaining subscriber data and data requested for the sole reason to identify the person (EPO)

– **REGULAR CASE IN OBTAINING TRAFFIC AND CONTENT DATA IN A DOMESTIC CASE**

The procedure for traffic and content data in a case classified as 'domestic' mirrors that of the first category (as outlined above). There is **no anticipated involvement from the enforcing authority**; instead, the provider is responsible for directly transferring the data to the issuing authority, with a deadline of no later than **10 days** under ordinary circumstances.

345 Regulation (EU) 2023/1543, Article 10(3) and (4).

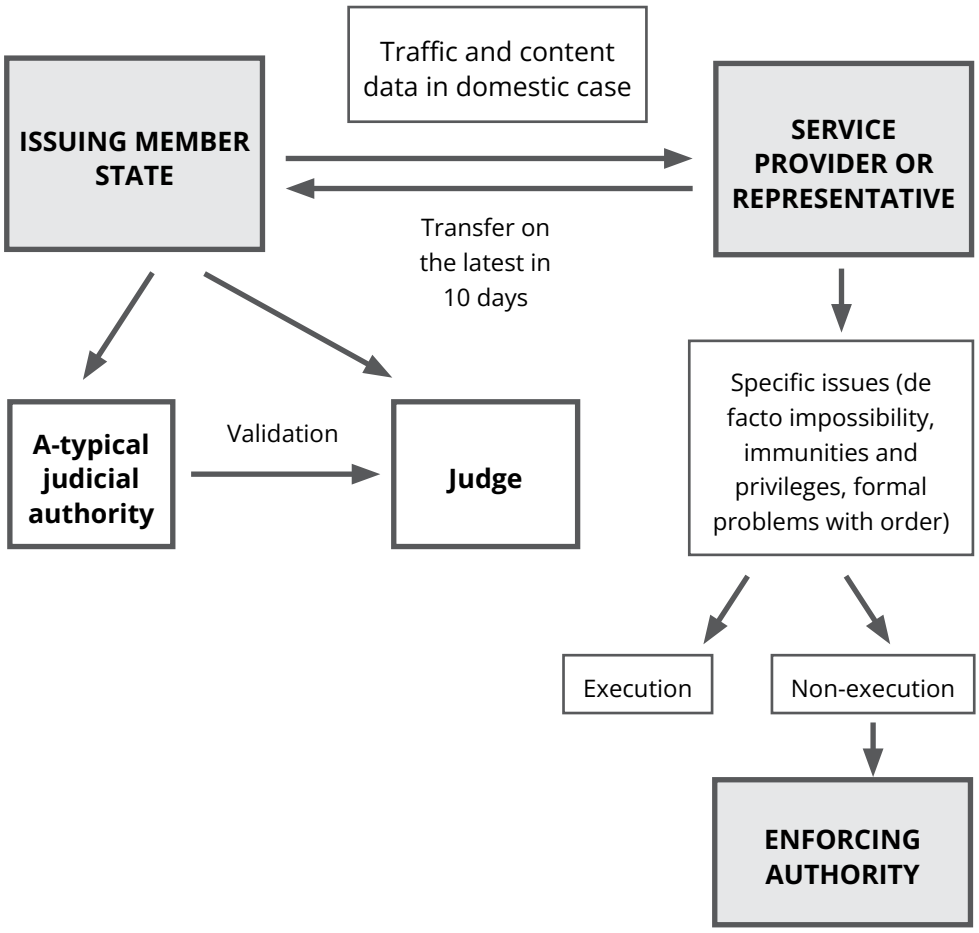

Figure 11: Regular Case in Obtaining Traffic and Content Data in a Domestic Case (EPO)

– **REGULAR CASE IN OBTAINING TRAFFIC AND CONTENT DATA IN A NON-DOMESTIC CASE, AND NOTIFICATION PROCEDURE WITH NON-RECOGNITION GROUNDS**

In cases involving **traffic and content data that are classified as non-domestic**, a special procedure more like the EIO is foreseen. In these scenarios, **the enforcing authority is also addressed through notification**.[346] However, unlike the EIO process, a formal approval from the enforcing authority is not required for the procedure to proceed. Should the enforcing authority not respond within the stipulated timeframe, their **silence is interpreted as consent**. Practically, this means that the service provider must wait for **10 days** for any communication from the enforcing authority before acting, unless notified earlier. Upon receiving the notification, the enforcing authority may invoke one of the non-recognition grounds specified in the Regulation. A significant point of discussion has been the mandatory or discretionary nature of these grounds. While the Framework Decision 2002/584/JHA on the European Arrest Warrant establishes mandatory and discretionary grounds[347], later mutual recognition instruments like the EIO have treated them as discretionary ('may' clause). The final text uses the phrasing: 'shall … assess the information and, where appropriate, raise one or more of the grounds,'[348] indicating that although the

346 Regulation(EU)2023/1543, Articles 8, 12.

347 Articles 3 and 4 of Framework Decision 2002/584/JHA, Articles 3, 4.

348 Regulation(EU)2023/1543, Article 12(1), introductory part.

judicial authority has the final say, there are circumstances where invoking a certain ground may be the only appropriate action. The scope of non-recognition grounds under this framework is narrower than in the EIO. Specifically, the non-recognition grounds are limited to situations where the requested action:

NON-RECOGNITION GROUNDS
a) The data requested are protected by immunities or privileges granted under the law of the enforcing State which prevent the execution or enforcement of the order, or the data requested are covered by rules on the determination or limitation of criminal liability that relate to freedom of the press or freedom of expression in other media, which prevent the execution or enforcement of the order.
b) In exceptional situations, there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution of the order would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right as set out in Article 6 TEU and in the Charter.
c) The execution of the order would be contrary to the principle of ne bis in idem.
d) The conduct for which the order has been issued does not constitute an offence under the law of the enforcing State, unless it concerns an offence listed within the categories of offences set out in Annex IV, as indicated by the issuing authority in the EPOC, if it is punishable in the issuing State by a custodial sentence or a detention order for a maximum period of at least 3 years.

Table 6: Non-recognition grounds (EPO)

The privileges recognised in the process of executing a request under this legal framework are those established under the law of the enforcing State. Should the need arise to waive a privilege or immunity, the issuing authority can request the notified enforcing authority to contact without delay the relevant authority within the enforcing State to initiate this action. In cases where the authority to waive lies beyond the enforcing State, such as with another Member State, a third country, or an international organisation, the issuing authority is empowered to directly approach the concerned authority to request the waiver. This framework incorporates **a non-recognition ground based on fundamental rights, as outlined in Article 6 of the Treaty on European Union (TEU)**. This inclusion, mirroring that within the EIO, is crucial to address potential disparities with national constitutional standards. It is particularly significant considering some harmonisation directives related to procedural rights that set minimal standards, such as those concerning the right to legal representation. Additionally, **the traditional approach to double criminality, excluding the list of 32 offences where it does not apply, is maintained**.[349] Should the enforcing authority identify a legitimate ground for refusal, it is required to notify both the addressee and the issuing authority,

349 Regulation (EU) 2023/1543, Annex IV,

effectively preventing the data transfer. Before invoking a refusal ground, the enforcing authority should engage with the issuing authority to discuss possible resolutions. **The enforcing authority has the discretion to oppose the transfer entirely, partially, or to stipulate specific conditions for the data's use.**

1. participation in a criminal organisation	17. racism and xenophobia
2. terrorism	18. organised or armed robbery
3. trafficking in human beings	19. illicit trafficking in cultural goods, including antiques and works of art
4. sexual exploitation of children and child pornography	20. swindling
5. illicit trafficking in narcotic drugs and psychotropic substances	21. racketeering and extortion
6. illicit trafficking in weapons, munitions and explosives	22. counterfeiting and piracy of products
7. corruption	23. forgery of administrative documents and trafficking therein
8. fraud, including fraud and other criminal offences affecting the Union's financial interests as defined in Directive (EU) 2017/1371 of the European Parliament and of the Council	24. forgery of means of payment
9. laundering of the proceeds of crime	25. illicit trafficking in hormonal substances and other growth promoters
10. counterfeiting currency, including the euro	26. illicit trafficking in nuclear or radioactive materials
11. computer-related crime	27. trafficking in stolen vehicles
12. environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties	28. rape
13. facilitation of unauthorised entry and residence	29. arson
14. murder or grievous bodily injury	30. crimes within the jurisdiction of the International Criminal Court
15. illicit trade in human organs and tissue	31. unlawful seizure of aircraft or ships
16. kidnapping, illegal restraint or hostage-taking	32. sabotage

Table 7: Offences in Article 12(1)(d) Regulation (EU) 2023/1543 where no double criminality check applies

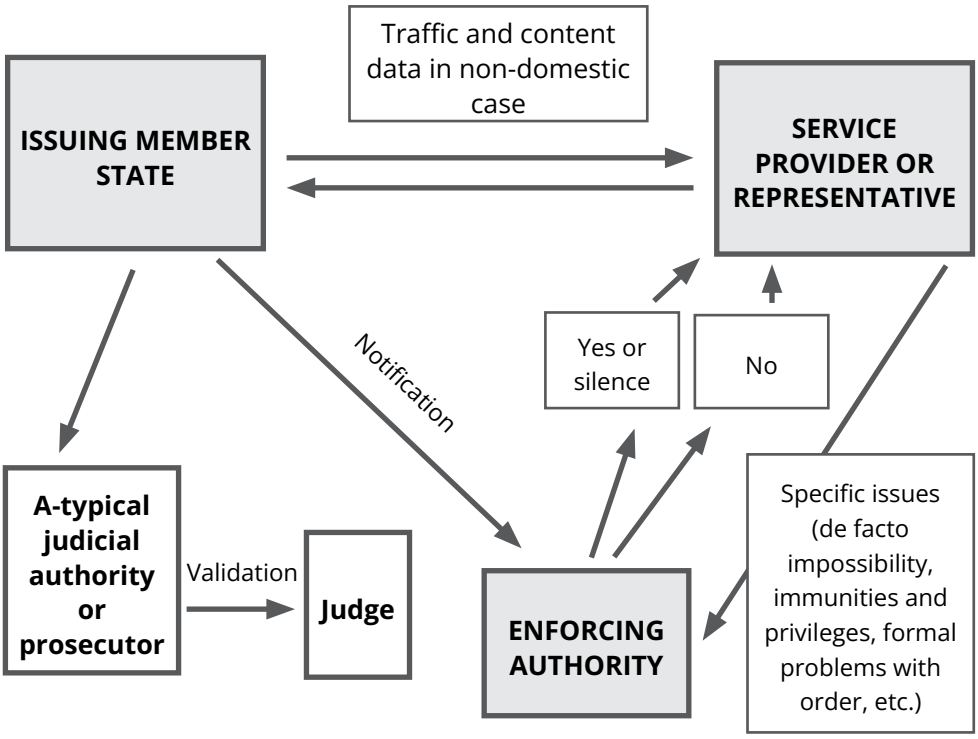

Figure 12: Regular Case in Obtaining Traffic and Content Data in a Non-domestic Case (EPO)

6.3.3.8. Emergency Cases

'Emergency cases' are defined as **situations in which there is threat to the life, physical integrity or safety of a person, or to a critical infrastructure, where the disruption or destruction of such critical infrastructure would result in an imminent threat to the life, physical integrity or safety of a person** through a serious harm to the provision of basic supplies to the population or the exercise of the core functions of the State.[350] In such cases, a reduced **deadline of 8 hours** is set, in contrast to the standard 10-day period. This expedited timeline **applies also in non-domestic cases for traffic and content data, where *ex-post* notification is required**. Following such *ex-post* notification, the **enforcing State has a window of 96 hours** to either object to the use of the data and request its deletion, or to conditionally agree to its use.[351] This approach draws inspiration from Article 31(3)(b) of Directive 2014/41/EU on the EIO, specifically regarding procedures for wiretappings conducted without the technical assistance of the executing State.

350 Regulation (EU) 2023/1543, Article 3, point 18.

351 Regulation (EU) 2023/1543, Article 10(4).

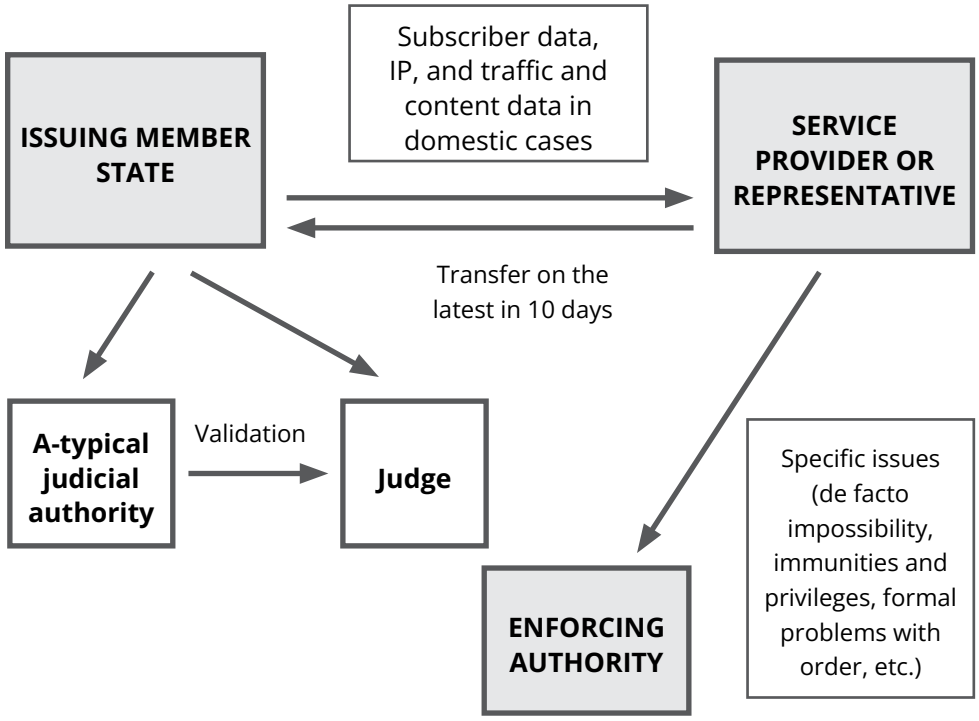

Figure 13: Urgent cases for subscriber data, IP addresses, and traffic and content data in domestic cases (EPO)

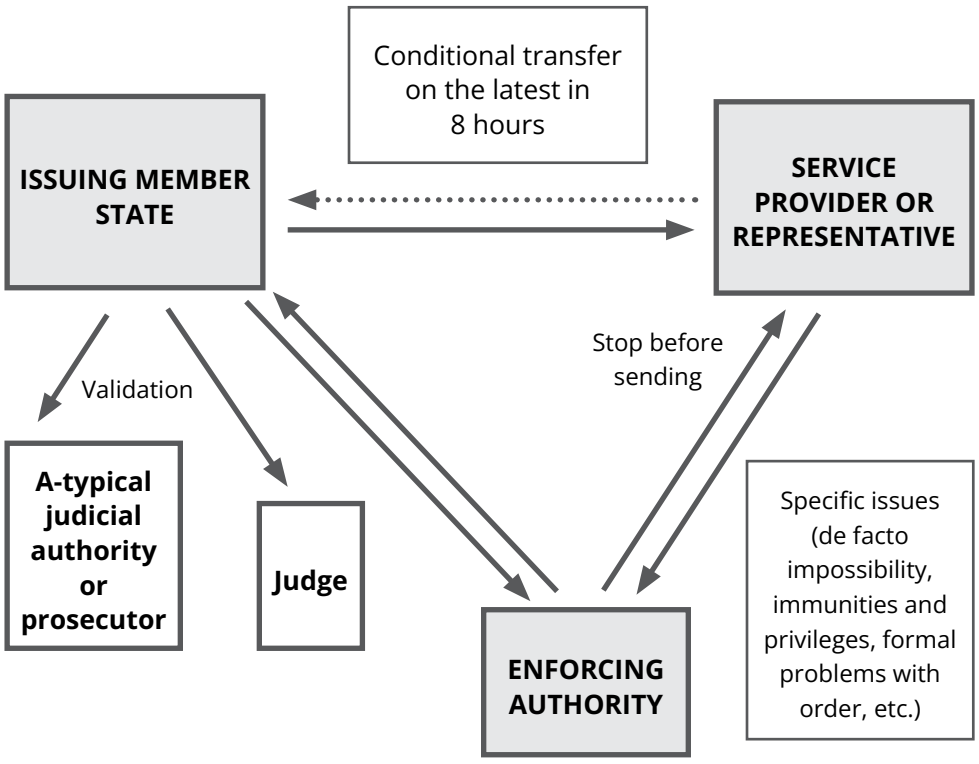

Figure 14: Urgent cases for traffic and content data in non-domestic cases (EPO)

6.3.3.9. Enforcement Procedure

In principle, **the enforcing authority in the second State becomes involved only if the provider opposes the Order**. In such a case, the enforcing authority should evaluate the matter within **5 working days** and either confirm the Order or refuse it. The enforcing authority is required to formally instruct the addressee to fulfil their relevant obligations, informing them of the ability to object to the Order, the penalties for non-compliance, and the deadline for either compliance or objection. The enforcement of the Order may be denied only based on one or more of the following grounds:

a. the Order has **not been issued or validated by an issuing authority** as provided for in Article 4;
b. the Order has **not been issued for an offence provided for in Article 5(4)**;[352]
c. the addressee could not comply with the certificate because of a ***de facto* impossibility** due to circumstances not attributable to the addressee, or because the certificate contains manifest errors;
d. the Order **does not concern data stored by or on behalf of the service provider** at the time of receipt of the certificate;
e. the **service is not covered by the Regulation**;
f. the data requested are **protected by immunities or privileges** granted under the law of the enforcing State, or the data requested are covered by rules on the determination or limitation of criminal liability that relate to **freedom of the press or freedom of expression** in other media, which prevent execution or enforcement of the Order;
g. in exceptional situations, based on the sole information contained in the EPOC, it is apparent that there are substantial grounds to believe, based on specific and objective evidence, that the execution of the European Production Order would, in the particular circumstances of the case, entail **a manifest breach of a relevant fundamental right as set out in Article 6 TEU and the Charter**.

Before deciding not to recognise or not to enforce the European Production Order or the European Preservation Order the enforcing authority shall consult the issuing authority by any appropriate means. Where appropriate, it shall request further information from the issuing authority. The issuing authority shall reply to any such request within 5 working days. The enforcing authority shall notify all its decisions immediately to the issuing authority and to the addressee. If the enforcing authority obtains the data requested by a European Production Order from the addressee, it shall transmit those data to the issuing authority without undue delay. Where the addressee does not comply with its obligations under a recognised European Production Order or European Preservation Order the enforceability of which has been confirmed by the enforcing authority, that authority shall impose a pecuniary penalty.

6.3.3.10. Conflicts of Third Country Laws

The **new system extends extraterritorially, binding third-country providers that offer services in the EU**, and even if the data is stored outside

352 This point does not apply to Preservation Orders. We presented together Article 16(4) and (5) of Regulation (EU) 2023/1543.

the EU. This setup raises the possibility of conflicts with third-country laws, potentially placing providers in situations of conflicting obligations regarding data disclosure. To address this, **a special procedure is envisaged specifically for European Production Orders**, but not for Preservation Orders.[353] Specifically, if **within 10 days of receiving an Order**, the provider or its legal representative determines that complying with a European Production Order would contravene obligations under the law of a third country, they are required to submit **a reasoned objection** to both the issuing and enforcing authorities, detailing the conflict with the third-country's law. It is important to note that neither the non-existence of similar provisions in the third country's law concerning the issuance of Production Orders nor the mere fact that data is stored in a third country constitutes a valid reason for non-compliance. Following the submission of an objection, the issuing authority must reassess the European Production Order, considering the objection and any feedback from the enforcing State. If the issuing authority decides to maintain the Order, it must seek a **review by the competent court within the issuing State**. This process suspends the execution of the European Production Order until the review is completed. However, the **timelines for this review process are determined by national law** and are not subject to harmonisation.

The competent court is tasked with determining whether a conflict of obligations exists between a European Production Order and the laws of a third country. This determination involves assessing whether the third country's law applies to the case at hand and whether, under these specific circumstances, it prohibits the disclosure of the requested data. If no conflict is found, the court will uphold the Order. However, if a conflict is identified, the court must decide whether to uphold or lift the European Production Order, considering several factors:

a. the **interest protected by the relevant law of the third country**, including fundamental rights as well as other fundamental interests preventing disclosure of the data, in particular national security interests of the third country;
b. the **degree of connection between the criminal case** for which the European Production Order was issued **and either of the two jurisdictions** (the location, nationality and place of residence of the person whose data are being requested or of the victim or victims of the criminal offence in question, the place where the criminal offence in question was committed);
c. the **degree of connection between the service provider and the third country** in question; in this context, the data storage location alone shall not suffice for the purpose of establishing a substantial degree of connection;
d. the **interests of the investigating State in obtaining the evidence** concerned, based on the seriousness of the offence and the importance of obtaining evidence in an expeditious manner;
e. the **possible consequences for the addressee** or for the service provider of complying with the European Production Order, including the potential penalties.

Although information from the third country may be sought, especially when fundamental rights or national security interests are at stake, it is not mandatory. If the court opts to lift the European Production Order, it must notify both the issuing authority and the addressee. Conversely, if the Order is

353 Regulation (EU) 2023/1543, Article 17.

upheld, the addressee is instructed to execute the Order, and the issuing authority is responsible for informing the enforcing authority of the review's outcome.

6.3.3.11. Legal Remedies

The Regulation provides legal remedies for affected persons (whether suspects or third parties) exclusively in the context of European Production Orders. It stipulates that if the affected person is a suspect or accused, they are entitled to effective remedies during the criminal proceedings where the data were used. This provision does not affect other remedies available under national law (including for Preservation Orders) or data protection remedies under Regulation (EU) 2016/679 (GDPR) and Directive (EU) 2016/680. In terms of the allocation of remedies between the issuing and enforcing States, the approach mirrors that of the European EIO system. **Substantive challenges to the measure, including questions of its legality, necessity, and proportionality, must be brought before a court in the issuing State according to its national law, without affecting fundamental rights guarantees in the enforcing State.** Individuals shall be timely informed about their right to a remedy, with consideration given to confidentiality requirements and the effectiveness of the remedy. Additionally, the Regulation introduces a fairness test for assessing admissibility, ensuring the rights of defence and the fairness of proceedings are upheld.[354]

CHECKLIST OF KEY POINTS ON THE SECOND ADDITIONAL PROTOCOL TO THE CONVENTION ON CYBERCRIME

- ☐ A European Production Order or a European Preservation Order may only be used in on-going criminal proceedings, strictly defined, or for tracking an absconding person, provided that the decision was not rendered in absentia, and the detention order is at least 4 months.
- ☐ These Orders are designated solely for obtaining historical evidence and are not applicable for real-time interception.
- ☐ Both prosecution and defence parties are permitted to use these Orders.
- ☐ It is crucial to verify that the telecommunication data being requested falls within the scope of the Regulation. Check Annex I, Section F, of Regulation (EU) 2023/1543 for common examples of data categories covered.
- ☐ Determine whether the case qualifies as 'domestic' using criteria such as the presence of a residence permit, family ties, bank accounts, telephone subscriptions, etc. In cases of uncertainty, treat the case as 'non-domestic' to avoid issues with the admissibility of evidence.
- ☐ Ensure that the issuing authority is either a prosecutor or a judge, noting that the national status of a prosecutor does not affect this requirement.

354 Regulation (EU) 2023/1543, Article 18.

- ☐ If the issuing authority is a police force or an investigative body, the Order must be validated by a national prosecutor or judge prior to being sent.
- ☐ In the event of an emergency case, carefully assess the situation before proceeding without prior validation. Adhere to the 48-hour deadline for obtaining *ex-post* validation. If validation is not forthcoming, consider refraining from using the obtained evidence. Alternatively, ensure any use of such evidence aligns with national rules on evidence admissibility.
- ☐ Enforcing authorities must be officially designated within the national legal framework as responsible for managing specific categories of electronic data, as precisely defined by national law.
- ☐ Carefully check all the conditions for issuing a European Production Order or a European Preservation Order, such as proportionality, prohibition of forum shopping, catalogue offence, whether the type of data is limited to certain offences, and the existence of possible privileges and immunities.
- ☐ Use the certificates from Annex I and III of Regulation (EU) 2023/1543 to transmit the Orders. Fill in the certificate diligently. Be aware that different addresses require different data, a shorter kind of certificate for providers and a more extensive one for enforcement authorities.
- ☐ Be aware that the provider might contact you to point out certain issues (technical problems, proportionality issues, indications of privileges, obvious mistakes). Take such input seriously and correct the certificate if necessary.
- ☐ As the enforcement authority, take notifications seriously as they refer to the most sensitive telecommunication data. Use non-recognition grounds carefully but use them if necessary.
- ☐ If evidence was already transferred in urgent circumstances, where a notification takes place, be aware that you can be legally co-responsible for any misuse of the data. If necessary, use the possibility to request deletion or limitation of such data within the provided time limit of 96 hours.
- ☐ As the enforcement authority, take objections from providers seriously and, if necessary, use the rejection grounds in the enforcement procedure. Keep the issuing authority informed about your procedures in that regard.
- ☐ Do not misuse the emergency procedure, as it might affect the admissibility of your electronic evidence.
- ☐ Provide affected persons with information on legal remedies as soon as possible, and do not impose unnecessary confidentiality regarding informing the affected person.
- ☐ Maintain communication with the other State to inform them about the legal remedies employed by the affected person in your country.
- ☐ Full content-based assessment of the measure must take place in the issuing State. In the executing State, legal remedies should be restricted to the procedural aspects of the measure within its territory, as well as issues related to fundamental rights.

6. CONCLUSION

The Toolkit is intended for practitioners seeking a basic overview of electronic evidence issues in connection with defence rights, specifically the presumption of innocence and the new EU cross-border evidence system. It offers readers fundamental insights into electronic evidence, including information on major EU and Council of Europe instruments, the different forms of cross-border co-operation, the definition of electronic evidence and telecommunication data, the life cycle of electronic evidence, and technical issues and terminology, such as 'the chain of custody'. It continues with a presentation of specific aspects of the presumption of innocence, mainly the burden of proof, the privilege against self-incrimination, and the right to remain silent, as well as the right to privacy. In this regard, a short overview of EU harmonisation instruments is provided. More specifically, in relation to the aforementioned right to remain silent, national systems display significant divergences regarding electronic evidence, for example, in terms of disclosure of passwords, bulk data collection, and access to files for suspects.

Furthermore, an analysis of the different procedural stages in dealing with electronic evidence is provided. In this context, particular attention is given to the pre-trial investigation, including the role of law enforcement in handling electronic evidence (for example, the legality and authenticity of collected evidence, the aforementioned chain of custody, etc.), and the role of different actors at this stage of the procedure, including defence lawyers. This is followed by an analysis of the judicial assessment phase of electronic evidence at trial. Here, the common EU standards on admissibility are assessed, with a specific focus on cross-border admissibility and proposing to the practitioners certain guidance. Finally, a more detailed presentation of the current EIO system is provided, with a special emphasis on cross-border electronic evidence gathering, as well as the new EU e-evidence system, introducing European Production Orders and European Preservation Orders, and based on Regulation (EU) 2023/1543 and Directive (EU) 2023/1544. The new system marks a new phase in the development of mutual recognition and digitalisation of cross-border criminal law cooperation in the EU. At the same time, it raises issue in view of its extraterritorial scope. As the system is not yet applicable, a general overview is provided, highlighting certain potential practical issues. Each chapter concludes with a reader-friendly checklist, offering the reader clear guidance and a summary of the most important issues to focus on.

Acknowledgements

Our thanks go to our fellow ZRS colleagues Judge **Martin Jančar**, **Erazem Bohinc**, **Rade Trivunčević**, **Ana Šajn**, as well as technical editors Mrs **Alenka Obid** and Mrs **Barbara Pandev**, for their time and contributions to this publication. We would also like to thank Mrs **Denitsa Kozhuharova** for her excellent coordination of the INNOCENT project, and our colleagues from partner institutions for their fruitful cooperation throughout the project. Special thanks must also go to **Martyna Kusak** for reading the Toolkit and providing valuable feedback.

ACRONYMS

APFS	Apple File System
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CoE	Council of Europe
CoE MLA Convention	European Convention on Mutual Assistance in Criminal Matters
CPT	European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment
DNA	Deoxyribonucleic acid
ECHR	European Convention on Human Rights
e-CODEX	e-Justice Communication via Online Data Exchange
ECtHR	European Court of Human Rights
EEW	European Evidence Warrant
EIO	European Investigation Order
EIO-LAPD Project	European Investigation Order - Legal Analysis and Practical Dilemmas of International Cooperation project
EJN	European Judicial Network
EPO	European Production Order
EPOC	European Production Order Certificate
EPOC-PR	European Preservation Order Certificate
EU	European Union
EVIDENCE project	European Informatics Data Exchange Framework for Courts and Evidence project
EVIDENCE2e-CODEX project	Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe project
Ext4	Fourth Extended Filesystem
F2FS	Flash-Friendly File System
FAIR project	Enhancing the Fair Trial for People Suspected or Accused of Crimes project
FORMOBILE project	From mobile phones to court – A complete FORensic investigation targeting mobile devices project
FRA	European Union Agency for Fundamental Rights

GDPR	General Data Protection Regulation
INNOCENT project	Improving the application of the presumption of iNNOCENce when applying elecTronic evidence project
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
JHA	the Justice and Home Affairs
JUST	Justice Programme
LEA	Law Enforcement Agency
MLA	Mutual Legal Assistance
MS	Member State
NGO	Non-Governmental Organisation
PIN	Personal Identification Number
PRESENT project	Enhancing the Right to be Present project
PROCAM project	Procedural Rights Observed by the Camera: Audiovisual Recordings of Interrogation in the EU project
QNX	Quantum Software Systems
QNX6	Quantum Software Systems Release 6
RAM	Random Access Memory
SQLite	Structured Query Language Lite
T-CY	Cybercrime Convention Committee
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TITANIUM project	Tools for the Investigation of Transactions in Underground Markets project
UK	United Kingdom
USA	United States of America
USB	Universal Serial Bus

LIST OF FIGURES AND TABLES

REFERENCES

Bibliography

Alegrezza, A. (2010). Critical Remarks on the Green Paper on Obtaining Evidence in Criminal Matters from one Member State to another and Securing its Admissibility. Zeitschrift für Internationale Strafrechtsdogmatik, Vol. 5, No 9/2010, pp. 569–579.

Antwi-Boasiako, A., Venter, H. (2017). A Model for Digital Evidence Admissibility Assessment. 13th IFIP International Conference on Digital Forensics (DigitalForensics), Orlando, FL, United States, pp. 23–38.

Best Practice Handbook. Enhancing the Fair Trial for People Suspected or Accused of Crimes (FAIR), (2018-2019), D2.4, pp. 1-51. https://www.netlaw.bg/p/f/a/fair-best-practices-handbook-en-2374.pdf, 23.3.2024.

Best practices for EUROpean COORDination on investigative measures and evidence gathering. EuroCoord, D4.3 (2019). pp.1-212. https://www.ejn-crimjust.europa.eu/ejn/libdocumentproperties/EN/3680, 23.3.2024.

Biasiotti, M. A. (2017). A proposed electronic evidence exchange across the European Union. Digital Evidence and Electronic Signature Law Review, 14, pp. 1–12. https://journals.sas.ac.uk/deeslr/article/view/2337/2289, 23.3.2024.

Birrer, A. (et al.) (May 2023). The state is watching you—A cross-national comparison of data retention in Europe. Telecommunications Policy, Vol. 47, No 4, May 2023.

Bonačić, M. (2022). Pristup elektroničkim dokazima: na putu prema novom modelu kaznenopravne suradnje u EU. Zagreb: Hrvatska akademija znanosti i umjetnosti, pp. 71–97.

Case-law by the Court of Justice of the European Union on the European Arrest Warrant. Eurojust. (2023). pp. 93–101. https://www.eurojust.europa.eu/publication/case-law-court-justice-european-union-european-arrest-warrant-october-2023, 23.3.2024.

Casey, E. (2010). Handbook of Digital Forensics and Investigation. California: Elsevier.

Christakis, T. (2020). E-Evidence in the EU Parliament: Basic Features of Birgit Sippel's Draft Report, European Law Blog, 2020.

Communication on Digitalisation of justice in the European Union – A toolbox of opportunities. (2.12.2020). European Commission, Brussels. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020DC0710, 23.3.2024.

Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses: overview of relevant court decisions and developments. Cybercrime Convention Committee, T-CY(2018)26. https://rm.coe.int/t-cy-2018-26-ip-addresses-v6/16808ea472, 25.3.2024.

Daniel, L. E., (2012). The Foundations of Digital Forensics: Best Practices. IN: Chap- ter 4.: Digital Forensics for Legal Practitioners: Understanding Digital Evidence From The Warrant To The Courtroom. California: Elsevier, pp.25–32. https://www.sciencedirect.com/science/article/abs/pii/B9781597496438000043, 23.3.2024.

Enhancing the Fair Trial for People Suspected or Accused of Crimes. Best Practices Handbook. FAIR Project (Start date 1 October 2018), https://www.netlaw.bg/p/f/a/fair-best-practices-handbook-en-2374.pdf, 22.3.2024.

Data retention across the EU. (July 2017). https://fra.europa.eu/en/publication/2017/data-retention-across-eu, 23.3.2024.

EIO-LAPD Project, Guidelines - European Investigation Order. (September 2021). https://lapd.pf.um.si/wp-content/uploads/2022/01/Guidelines_EN_final.pdf, 23.3.2024.

Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and Judges. (2020). Council of Europe (DGHRRL), pp. 151–153.

Electronic evidence in criminal matters. European Parliamentary Research Service, September 2023, pp. 1–12. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI(2021)690522_EN.pdf, 23.3.2024.

ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings. European Law Institute project description. (September 2020-May 2023). https://www.europeanlawinstitute.eu/projects-publications/completed-projects/admissibility-of-e-evidence/, 23.3.2024.

ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings: Draft Legislative Proposal of the European Law Institute, University of Vienna. European law Institute, 2023, pp.1-40. https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU-.pdf, 23.3.2024.

Enhancing the Fair Trial for People Suspected or Accused of Crimes (FAIR). European Commission, JUSTICE Programme project description, (October 2018- November 2020), https://www.netlaw.bg/en/a/enhancing-the-fair-trial-for-people-suspected-or-accused-of-crimes-fair, 23.3.2024.

Enhancing the Right to be Present (PRESENT). European Commission, JUSTICE Programme project description, (January 2018- December 2019). https://www.netlaw.bg/en/a/enhancing-the-right-to-be-present-present, 23.3.2024.

Erbežnik, A. (2014). Mutual Recognition in EU Criminal Law and Its Effects on the Role of a National Judge. IN: Peršak, N. Legitimacy and Trust in Criminal Law, Policy and Justice Ashgate: Routledge.

Erbežnik, A. (2023). New EU system on cross-border gathering of e-evidence – analysis and open questions. Dignitas, No 98, pp. 47–72.

Erbežnik, A. (2024). International Encyclopaedia of Laws, EU Criminal Law. Alphen aan den Rijn: Kluwer.

Erbežnik, A., Bonačić, M. European Investigation Order, E-Evidence and the Future of Cross-Border Cooperation in the EU. IN: Ambos, K. (et al.) (2023). The European Investigation Order Legal Analysis and Practical Dilemmas of International Cooperation, Berlin, pp. 243–262.

Erbežnik, A., Dežman Z. (2022). Introduction to Criminal Procedure Law [Uvod v kazesko procesno pravo]. Ljubljana: GV Založba, Lexpera.

EU Directive on the Presumption of Innocence: Implementation Toolkit. (2017). Legal Experts Advisory Panel, Fair Trials, Roadmap practitioner tools, pp. 1–35. https://www.fairtrials.org/app/uploads/2022/01/Presumption-of-Innocence-Toolkit_2.pdf, 23.3.2024.

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14. (4 November 1950). Council of Europe, ETS 5, pp. 1–34. https://www.echr.coe.int/documents/d/echr/convention_ENG, 23.3.2024.

European Informatics Data Exchange Framework for Courts and Evidence (EVIDENCE). (2022).

European Commission, CORDIS EU research results. http://www.evidenceproject.eu/, 23.3.2024.

EVIDENCE2e-CODEX – Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe. (15.2.2018- 14.2.2020). European Commission, JUSTICE Programme project description, https://evidence2e-codex.eu, 23.3.2024.

FOREnsic evidence gathering autonomous seNSOR. FORENSOR project description. (September 2015-February 2019). European Commission, CORDIS EU research results, https://cordis.europa.eu/project/id/653355, 23.3.2024.

Forlani, G. (2023). The E-evidence Package: The Happy Ending of a Long Negotiation Saga. Eucrim, Focus: Electronic Evidence, 2/2023, pp. 174–181.

FORMOBILE Guidance to Checklist Preparation for Legal Practitioners. (2022). European Commission, CORDIS EU research results.

From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices (FORMOBILE). (26 April 2019). European Commission, CORDIS EU project description, https://cordis.europa.eu/project/id/832800, 23.3.2024.

The Criminal Procedure Report, FORMOBILE, From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices, (December 2022), D2.2., pp. 1–144.

Garamvölgyi, B., Ligeti, K., et al. (2021). Admissibility of E-Evidence in Criminal Proceedings in the EU. Eucrim, Focus: The Future of EU Criminal Justice – Expert Perspectives, 3/2020, pp. 201-208. https://eucrim.eu/articles/admissibility-evidence-criminal-proceedings-eu/, 23.3.2024.

Granja, F. M., Rafael, G. D. (2017). The preservation of digital evidence and its admissibility in the court. International Journal of Electronic Security and Digital Forensics, 9(1), p. 118.

Guide on Article 6 of the Convention – Right to a fair trial (criminal limb). Council of Europe, (2014), http://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf, 23.3.2024.

Hoffer, J. (2024). The Ongoing Legal Battle: Biometrics, 5th Amendment, and Phone Decryption. The Berkeley Table. https://medium.com/the-berkeley-table/the-ongoing-legal-battle-biometrics-5th-amendment-and-phone-decryption-8353c6f-2f81a, 23.3.2024.

Hummert, Ch., Pawlaszcyk D. (2022). Mobile Forensics – The File Format Handbook. Common File Formats and File Systems Used in Mobile Devices. FORMOBILE. Cham: Springer. https://link.springer.com/book/10.1007/978-3-030-98467-0, 23.3.2024.

Impact Assessment – Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence.

INNOCENT Report (DRAFT). (2023). INNOCENT – Improving the presumption of innocence when handling electronic evidence. WP2: Comparative Analysis of Data, D.2.1, prepared by the Adam Mickiewicz University Poznań.

Joint Note of Eurojust and the EJN on the practical application of the European Investigation Order. European Union Agency for Criminal Justice Cooperation, (2019), p.1-18. https://www.eurojust.europa.eu/publication/joint-note-eurojust-and-ejn-practical-application-european-investigation-order, 23.3.2024.

Kusak, M. (2016). Mutual admissibility of evidence in criminal matters in the EU. A study of telephone tapping and house search. Institute for International Research on Criminal Policy. Apeldoor, Antwerp, Portland: Maklu.

Kusak, M. (2017). Common EU Minimum Standards for Enhancing Mutual Admissibility of Evidence Gathered in Criminal Matters. European Journal on Criminal Policy and Research, v. 23, pp. 337–352.

Kusak, M. (2019). Mutual admissibility of evidence and the European investigation order: aspirations lost in reality. ERA Forum. Journal of the Academy of European Law, 19(3), pp. 391–401.

Lasser, M. (2009). Judicial Deliberations: A Comparative Analysis of Transparency and Legitimacy. Oxford Studies in European Law.

Legality check of SKY-ECC evidence is mandatory. Italian Supreme Court, nr. 44154/23, (7.11.2023), https://canestrinilex.com/en/readings/legality-check-of-skyecc-evidence-is-mandatory-ita-supreme-court-4415423, 20.1.2022.

McBride, J. (2018). The case law of the European Court of Human Rights on Evidentiary standard in criminal proceedings. Council of Europe, pp.1–26. https://rm.coe.int/council-of-europe-georgia-european-court-of-human-rights-case-study-ev/16807823c3, 23.3.2024.

Mobile phone data extraction by police forces in England and Wales Investigation report. (2020). Information Commissioner's Office, Version 1.1. https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf, 23.3.2024.

Novak, M., Grier, J., Gozales, D. (2018). New approaches to digital evidence acquisition and analyses. National Institute of justice Journal, pp. 1–8. https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis, 23.3.2024.

Overview of existing legal framework in EU Member States. (30.10.2015). European Commission, CORDIS EU research results. European Informatics Data Exchange Framework for Courts and Evidence (EVIDENCE), D3.1, pp.1–145. http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d3-1-411.pdf, 23.3.2024.

Presumption of innocence and related rights – Professional perspectives (31.3.2021). European Union Agency for Fundamental Rights, pp.1–104. https://fra.europa.eu/en/publication/2021/presumption-of-innocence, 23.3.2024.

ProCam – Procedural Rights Observed by the Camera: Audiovisual Recordings of Interrogation in the EU. (1.9.2017-30.6.2019). European Commission, JUSTICE Programme project description, https://www.oijj.org/en/our-work/research/projects/procam-procedural-rights-observed-camera-audiovisual-recordings, 23.3.2024.

ProCam – Procedural Rights Observed by the Camera: Audiovisual Recordings of Interrogation in the EU. European Commission, JUSTICE Programme project description, 1.9.2017–30.6.2019.

Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. (2018). European Commission, Commission Staff Working Document, https://eur-lex. europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN, 23.3.2024.

Raburu, G., Dinga, L. (2020). Legal Issues in Computer Forensics and Digital Evidence Admissibility. International Journal of Computer Science and Mobile Computing, vol. 9(7), pp. 86–89. https://ijcsmc.com/docs/papers/July2020/V9I7202021.pdf, 23.3.2024.

Ramadhan, R. A., Setiawan, P. R., Hariyadi, March D. (2012). Digital Forensic Investigation for Non-volatile Memory Architecture by Hibrid Evaluation Based on ISO/ESC 27307:2012 and NIST SP800-86 Framework. IT Journal Research and De- velopment (ITJRD), Vol. 6, No 2, pp. 163. http://journal.uir.ac.id/index.php/ITJRD, 23.3.2024.

Recommendation list. Enhancing the Right to be Present (PRESENT). (2019). D3.4, pp.1–23. https://www.netlaw.bg/p/r/e/recommendation-list-2467.pdf, 23.3.2024.

Report on data protection and other fundamental rights issues. EVIDENCE2e-CODEX – Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe. (2018-2019). European Commission, JUSTICE Programme, D2.3., pp.1–5. https://evidence2e-codex.eu/p/e/v/evidence2e-codex-deliverable-d2-3-summary-436.pdf, 23.3.2024.

Report on EIO and MLA. EVIDENCE2e-CODEX – Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe. (2018-2020). European Commission, JUSTICE Programme, D2.2, pp.1–3. https://evidence2e-codex.eu/p/e/v/evidence2e-codex-deliverable-d2-2-summary-731.pdf, 23.3.2024.

Report on Eurojust's casework in the field of the European Investigation Order. (November 2020). Eurojust, p.1–58. https://www.eurojust.europa.eu/sites/default/files/2020-11/2020-11_EIO-Casework-Report_CORR_.pdf, 23.3.2024.

Report on implementation of EIO. EVIDENCE2e-CODEX – Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe. (2018-2019). European Commission, JUSTICE Programme, D2.1, pp. 1–4. https://evidence2e-codex.eu/p/e/v/evidence2e-codex-deliverable-d2-1-summary-523.pdf, 23.3.2024.

Report on implementation of EIO. EVIDENCE2e-CODEX – Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe. (2018-2019). European Commission, JUSTICE Programme, D2.1, pp. 1–4.

Rights in practice: right to access to a lawyer and procedural rights in criminal and European arrest warrant proceedings. (2019). European Union Agency for Fundamental Rights, pp. 1–79. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-rights-in-practice-access-to-a-lawyer-and-procedural-rights-in-criminal-and-european-arrest-warrant-proceedings.pdf, 23.3.2024.

Risinger, D. M., Risinger, L. C. (2012). Innocence Is Different: Taking Innocence into Account in Reforming Criminal Procedure. New York Law School Law Review, 56(3), pp. 869–909. https://digitalcommons.nyls.edu/cgi/viewcontent.cgi?article=1663&context=nyls_law_review, 23.3.2024.

Roadmap. European Commission, CORDIS EU research results. European Infor- matics Data Exchange Framework for Courts and Evidence (EVIDENCE). (2022). D9.2, pp. 1–111. https://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d9-2-426. pdf, 23.3.2024.

ROXANNE – Real time network, text, and speaker analytics for combating organised crime European Commission, (September 2019- December 2022). Horizon 2020 Programme project description, https://roxanne-euproject.org, 23.3.2024.

T-CY Guidance Notes, Adopted by the 8th, 9th, 12th, 16th and 21st Plenary of the T-CY. (8 July 2019). Council of Europe, Strasbourg, pp. 1–38. https://rm.coe.int/t-cy-guidance-notes-compilation/16809fc22c, 23.3.2024.

Simonato, M. (2014). Defence rights and the use of information technology in criminal procedure. Revue internationale de droit pénal, 85(1-2), pp. 261–310.

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. Computer Law & Security Review, 42, pp. 1–20. https://doi.org/10.1016/j.clsr.2021.105575, 23.3.2024.

Stoykova, R. (2023). Encrochat: The hacker with a warrant and fair trials? Forensic Science International: Digital Investigation, Vol. 46, pp.1–14. https://doi.org/10.1016/j.fsidi.2023.301602, 23.3.2024.

Summaries of EU legislation: Electronic evidence in criminal proceedings – designated establishments and legal representatives of service providers. (30.5.2023). EUR-Lex Acces to European Union Law, https://eur-lex.europa.eu/EN/legal-content/summary/electronic-evidence-in-criminal-proceedings-designated-establishments-and-legal-representatives-of-service-providers.html, 23.3.2024.

Summaries of EU legislation: Mutual assistance in criminal matters between EU countries. (10.9.2018). EUR-Lex Acces to European Union Law, https://eur-lex.europa.eu/EN/legal-content/summary/mutual-assistance-in-criminal-matters-between-eu-countries.html, 23.3.2024.

Thaman, S. C. (2010). Fruits of the Poisonous Tree in Comparative Law. Southwestern Journal of International Law, v. 16, pp. 333–384.

The Criminal Procedure Report. (2022). European Commission, CORDIS EU research results.

Tinoco-Pastrana, A. (2020). The Proposal on Electronic Evidence in the European Union, eucrim, No 1, pp. 46–50.

Tools for the Investigation of Transactions in Underground Markets. TITANIUM project description. (May 2017- April 2020). European Commision, CORDIS EU research results, https://cordis.europa.eu/project/id/740558, 23.3.2024.

Tosza, S. (2018). The European Commission's Proposal on Cross-Border Access to E-Evidence, eucrim, No 4/2018, pp. 212–219.

Tosza, S. (2020). All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order, New Journal of European Criminal Law, Vol. 11, No 2, pp. 161–183.

Vaciago, G., Silva Ramalho, D. (2016). Online searches and online surveillance of trojans and other types of malware as means of obtaining evidence in criminal proceedings. Digital Evidence and Electronic Signature Law Review, 13, pp. 88–96.

Vermeulen, G. (2011). Free gathering and movement of evidence in criminal matters in the EU: Thinking beyond borders, striving for balance, in search of coherence. Apeldoor, Antwerp, Portland: Maklu.

Wahl, T. (2022). Encrochat Turns into a Case for the CJEU, Eucrim, No 3/2022, pp. 197–198.

Zubik, M., Podkowik, J., et al. (2021). European Constitutional Courts towards Data Retention Laws. Law, Governance and Technology Series, v. 45. Springer.

Case Law

CJEU. Åkerberg Fransson, C-617/1027, Judgment of the Court (Grand Chamber) of 26 February 2013.

CJEU. Direktor na Glavna direktsia 'Natsionalna politsia' pri MVR – Sofia, C-118/22, Judgment of the Court (Grand Chamber) of 30 January 2024.

CJEU. H.K., C-746/18, Judgment of the Court (Grand Chamber) of 2 March 2021.

CJEU. Kossowski, C-486/14, Judgment of the Court (Grand Chamber) of 29 June 2016.

CJEU. Kraaijenbrink, C-367/05, Judgment of the Court (Second Chamber) of 18 July 2007.

CJEU. La Quadrature du Net et al., C-511/18, Judgment of the Court (Grand Chamber) of 6 October 2020.

CJEU. Mantello, C-261/09, Judgment of the Court (Grand Chamber) of 16 November 2010.

CJEU. Spasic, C-129/14 PPU, Judgment of the Court (Grand Chamber), 27 May 2014.

CJEU. Staatsanwaltschaft Berlin (EncroChat). C-670/22, ongoing.

CJEU. Staatsanwaltschaft Wien v A. and Others, C-584/19, Judgment of the Court (Grand Chamber) of 8 December 2020.

CJEU. van Esbroeck, C-436/04, Judgment of the Court (Second Chamber) of 9 March 2006.

ECHR. Barberà, Messegué and Jabardo v. Spain, 6.12.1988, a. No 10590/83. ECHR. Aleksandr Zaichenko v. Russia, 18.2.2010, a. No 39660/02.

ECHR. Allan v. the United Kingdom, 28.8.2001, a. No 48539/99. ECHR. Benedik v. Slovenia, 24.4.2018, a. No 62357/14.

ECHR. Beuze v. Belgium, 9.11.2018, a. No 71409/10. ECHR. Dayanan v. Turkey, 13.10.2009, a. No 7377/03. ECHR. Dragojević v. Croatia, 15.1.2015 a. No 68955/11. ECHR. Dvorski v. Croatia, 20.10.2015, a. No 25703/11.

ECHR. Engel and Others v. Netherlands, 8.6.1976, a. Nos 5100/71, 5101/71, 5102/71, 5354/72, 5370/72.

ECHR. Gäfgen v. Germany, 1.6.2010, a. No 22978/05.

ECHR. Heaney and Meguiness v. Ireland, 21.12.2000, a. No 34720/97.

ECHR. Ibrahim and Others v. the United Kingdom, 13.9.2016, a. Nos 50541/08, 50571/08, 50573/08 and 40351/09.

ECHR. Iordachi and Others v. Moldova, 10.2.2009, a. No 25198/02. ECHR. Jalloh v Germany, 11.6.2006, a. No 54810/00.

ECHR. John Murray v. the United Kingdom, 8.2.1996, a. No 18731/81. ECHR. Khan v. United Kingdom, 12.5.2000, a. No 35394/97.

ECHR. Marcello Viola v. Italy, 5.10.2006, a. No 45106/04. ECHR. Minteh v. France, 31.5.2021, a. No 23624/10.

ECHR. Moiseyev v. Russia, 9.11.2008, a. No 62936/00. ECHR. Natunen v. Finland, 31.5.2009, a. No 21022/04. ECHR. Padalov v. Bulgaria, 10.11.2006, a. No 54784/00. ECHR. Panovits v. Cyprus, 11.12.2008, a. No 4268/04.

ECHR. S v. Switzerland, 28.11.1991, a. Nos 12629/87 and 13965/88.

ECHR. Salabiaku v. France, 7.10.1988, a. No 10519/83.

ECHR. Salduz v. Turkey, 27.11.2008, a. No 36391/02.

ECHR. Saunders v. the United Kingdom, 17.12.1996, a. No 19187/91.

ECHR. Schenk v. Switzerland, 12.6.1988, a. No 10862/84.

ECHR. Sigurður Einarsson and others v. Iceland, 4.6.2019, a. No 39757/15.

ECHR. Simeonovi v. Bulgaria, 12.5.2017, a. No 21980/04.

ECHR. Van Wesenbeeck v. Belgium, 23.5.2017, a. No 67496/10 and 52936/12.

ECHR. Yüksel Yalçınkaya v. Türkiye, 26.9.2003, a. No 15669/20. ECHR. Zličić v. Serbia, 26.1.2021, a. No 73313/17 and 20143/19. Slovenian Constitution Court, case No U-I-144/19, 6.6.2023.

Slovenian Constitutional Court, case No Up-1006/13, 9.6.2016. Slovenian Constitutional Court, case No Up-127/16, 20.1.2022. Slovenian Constitutional Court, case No Up-326/14, 6.12.2017.

Supreme Court of the Netherlands. 13 October 2020, ECLI:NL:HR:2021:202.

U.S. Supreme Court, Nardone v. United States, 11.12.1939, 308 U.S. 338.

U.S. Supreme Court, Silverthorne Lumber Co. v. United States, 26.1.1920, 251 U.S. 385.

Legislation

Council of Europe Law

Budapest Convention on Cybercrime: Benefits and Impact in Practice. Council of Europe, Strasbourg 13 July 2020, p. 1–45. https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac, 23.3.2024.

Convention on Cybercrime, Special edition dedicated to the drafters of the Convention (1997-2001). 2022. In 4. Explanatory report to the Convention on Cybercrime. Council of Europe, March 2022, p. 57–124. https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e, 23.3.2024.

Convention on Cybercrime. Council of Europe, ETS 185, 23 November 2001. https://www.refworld.org/legal/agreements/coe/2001/en/90189, 23.3.2024.

European Convention on Mutual Assistance in Criminal Matters. Council of Europe, ETS No. 030, 20 April 1959, p. 1–9. https://rm.coe.int/16800656ce, 23.3.2024.

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, Council of Europe, ETS 5, 4 November 1950, https://www.echr.coe.int/documents/d/echr/convention_ENG, 23.3.2024

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Council of Europe, CETS 224, 17 November 2021, p.1–21. https://rm.coe.int/1680a49dab, 23.3.2024.

Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters. Council of Europe, ETS No. 182, 8 November 2001, p.1–16. https://rm.coe.int/168008155e, 23.3.2024.

The Charter of the Fundamental Rights of the European Union, Official Journal of the European Communities, a. no. 364/01.

EU Law

Charter of Fundamental Rights of the European Union. Official Journal of the European Communities, 18 December 2000 (2000/C 364/01), p. 391–407. https://www.refworld.org/docid/3ae6b3b70.html, 23.3.2024.

Consolidated version of the Treaty on European Union, OJ C 326, 26.10.2012, pp. 13–390.

Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, pp. 47–390.

Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000, pp. 3–23.

Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ L C 197, 12.7.2000, pp. 3–23.

Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239, 22.9.2000, pp. 19–62.

Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, OJ L 350, 30.12.2008, pp. 144–164.

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241, 17.9.2015, pp. 1–15.

Directive (EU) 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, OJ L 65, 11.3.2016, pp. 1–11.

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, OJ L 119, 4.5.2016, pp. 89–131.

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, OJ L 119, 4.5.2016, pp. 89–131.

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88, 31.3.2017, pp. 6–21.

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, OJ L 321, 17.12.2018, pp. 36–214.

Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, OJ L 123, 10.5.2019, p. 18–29.

Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, OJ L 191, 28.7.2023, pp. 181–190.

Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17.12.2011, pp. 1–14.

Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European Protection Order, OJ L 338, 21.12.2011, pp. 2–18.

Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, OJ L 142, 1.6.2012, pp. 1–10.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, pp. 8–14.

Directive 2013/48/EU of the European Parliament and f the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, OJ L 294, 6.11.2013, pp. 1–12.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, pp. 1–36.

Directive 2016/343/EU of the European Parliament and f the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, OJ L 65, 11.3.2016, pp. 1–11.

Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office, (COM(2013) 534), Article 30(1). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52013PC0534, 23.3.2024.

Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. Explanatory memorandum, Council of Europe, Strasbourg, 17 April 2018.

Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), OJ L 150, 1.6.2022, p. 1.

Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. OJ L 191, 28.7.2023, pp. 118–180.

Regulation (EU) 2023/2844 on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation. OJ L, 2023/2844, 27.12.2023.

Resolution of the Council of 30 November 2009 on a Roadmap for strengthening the procedural rights of suspected or accused persons in criminal proceedings, OJ C 295, 4.12.2009, pp. 1–3.

Other

Criminal Procedure Act (CPA), Official Gazette of the Republic of Slovenia, a. No 176/21.

ABOUT THE AUTHORS

Benjamin Flander

Benjamin Flander is an Associate Professor of Law at the University of Maribor, Faculty of Criminal Justice and Security, and Senior Research Associate at the Law Institute of the Science and Research Centre Koper, Slovenia. He is an expert in theory of law, constitutional law and human rights in criminal justice systems, and the author of several scientific monographs and articles. He was an evaluator at the Group of States Against Corruption (GRECO) (4th evaluation round) and coordinated a national research project on the effectiveness of control over the police in the field of fundamental rights (2019-2021).

Anže Erbežnik

Anže Erbežnik is a Professor of Criminal Law and Criminology, European Faculty of Law, Slovenia. He is an expert in criminal law, criminal procedural law, constitutional criminal law, EU criminal law and judicial cooperation. He has extensive experience in the legislative process at EU level in the area of fundamental rights, justice and home affairs, and is author of several articles and monographs in that regard. He works for the European Parliament and is further specialising in AI law, and Law and Technology at the University of California, Berkeley.

REVIEWS

This book was written within the framework of the project INNOCENT - Improving the application of the presumption of innocence when applying electronic evidence, funded by the European Commission (JUST) and coordinated by the Law and Internet Foundation, Bulgaria. It was co-authored by Benjamin Flander, Associate Professor of Law at the Faculty of Criminal Justice and Security, University of Maribor and Senior Research Associate at the Law Institute of the Science and Research Centre Koper, Slovenia; Anže Erbežnik, Professor of Criminal Law at the European Faculty of Law, New University, Slovenia, and Administrator, Legal Affairs Committee, European Parliament.

Apart from the introductory section that addresses the INNOCENT project, its objectives, scope, and the book's structure, this publication comprises five main parts. The first part, an introductory section, pertains to existing projects and guidance documents on evidence in the digital age.

The second part provides a comprehensive and detailed overview of the intricate regulatory landscape governing electronic evidence within the European Union (EU) legal framework, encompassing primary legislation such as the Charter of Fundamental Rights of the European Union and secondary legislation on cooperation in criminal matters. It also delves into the Council of Europe's perspective in the context of human rights regulations, specifically the European Convention for the Protection of Human Rights, and the realm of cybercrime regulation. While this part itself doesn't analyse relevant case law in detail, the subsequent chapter focuses on the presumption of innocence and fair trial rights within the EU and Council of Europe legal frameworks, constituting a crucial step in electronic evidence analysis and includes also the case law references.

The fifth chapter delineates the definition, origins, types, and life cycle of electronic evidence, proposing a common legal framework and standardized procedures in this context.

The central sixth chapter integrates conclusions drawn from previous chapters and scrutinizes the procedural framework for managing and admitting electronic evidence in criminal proceedings, emphasizing the presumption of innocence and fair trial rights of suspects and accused individuals across different stages of criminal procedures.

The concluding seventh chapter provides a summary of the book's pivotal contributions, offering a fundamental grasp of issues encompassing electronic evidence in relation to defence rights, electronic evidence insights, cross-border cooperation mechanisms, electronic evidence definition, telecommunication data, evidence lifecycle, technical aspects, terminology, and specific facets of the presumption of innocence, the right to silence, the right to privacy, EU harmonization instruments, and procedural stages relating to electronic evidence.

While this book modestly emphasizes its relevance to practitioners including judges, prosecutors, defence lawyers, and legal aid practitioners, aiming to furnish them with essential knowledge on electronic evidence access, utilization, and transfer while prioritizing human rights protection, its significance surpasses its self-acknowledged role. Notably, it underscores the increasing presence of electronic evidence in contemporary digitalized societies and

criminal activities, underlining the necessity for practitioners in all criminal justice realms to comprehend the importance and risks associated with electronic evidence.

Furthermore, this book extends beyond practitioners, serving as a valuable resource for students, academics, and individuals engaging with electronic evidence, offering a profound and insightful analysis of electronic evidence usage in criminal procedures, international cooperation dynamics, and human rights considerations within the electronic evidence landscape.

In Ljubljana, 10 May 2024

Dr Sabina Zgaga Markelj,
Assistant Professor of Criminal law,
Adviser to the Constitutional Court of the Republic of Slovenia

Due to the rapid development of the technology, the bandling and admissibility of electronic evidence has been in scientific focus for some time. The latest development in this area is the Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. The Regulation lays down rules under which an authority of Member State can order a service provider in another Member State to produce or to preserve electronic evidence for the purposes of criminal proceedings and it will apply from 18 August 2026. It is a very current and relevant topic, which is additionally contributed by the fact that the topic is considered from the perspective of the procedural rights of suspects and defendants.

The manuscript (hereinafter: Toolkit) is a deliverable of the Innocent project founded by the EU, which aimed to enhance the application of the presumption of innocence when handling electronic evidence. Its target group are judges, prosecutors and defence lawyers (particularly those operating in Central and Eastem Europe) who encounter e-evidence in their work. In addition to these practitioners, the Toolkit will be interesting to anyone interested in e-evidence, especially students.

As stated in the Toolkit, its primary objective is to "to offer comprehensive guidance and enhance the skills and knowledge of judges, prosecutors, and defence lawyers concerning tbe procedura} rights of individuals suspected or accused of crimes. Specifically, it focuses on the fundamental right to be presumed innocent until proven guilty, particularly in criminal cases relying on electronic_evidence. The aim is to elevate comprehension of distinct legai and practical issues and challenges inherent in various phases of the electronic evidence life cycle. Furthermore, the Toolkit aspires to furnish practical guidance for handling electronic evidence throughout both the pre-trial and trial stages of criminal proceedings." (p. 10). In order to achieve its objectives, after the lntroduction and background (pp. 9-13), the Toolkit contains five chapters and a conclusion (p. 129). Chapter 2 presents key highlights from other projects and guidance documents (pp. 15-21) and Chapter 3 provides an overview of the intemational and EU legai framework in this area (pp. 23-45). The following two chapters deal with the electronic evidence. Chapter 5 covers the definition, types and 'life circle' of electronic evidence, as well as lays down legal framework for their handling and admissibility (pp. 57-64). Chapter 6 deals with procedural framework for handling and admissibility of electronic evidence in pre-trial investigation stage, at trial and with their cross-border access (pp. 65-128). It is accompanied by the executive summary (pp. 7-8), acronyms (pp. 130-131), list of schemes and tables (p. 132), references (pp. 133-142) and information about the authors (p. 143).

The methodology corresponds to the intended purpose of the publication. As stated, the Toolkit is based on reports created within the project, the results of other projects, the legai framework of the Council of Europe and the EU, case law of supranational and national courts, various reports related to electronic evidence and scientific literature. The Toolkit is written in a clear language, and it is easy to understand. The style corresponds to the purpose of the publication, and it complies with the rules of scientific writing, as well as bibliographic rules. The text itself uses text highlighting (holding and framing the text), schemes and tables, and each chapter and subchapter contains a checklist of key points. The Toolbox tries to combine the providing of basic information

about the intemational and EU legal framework, the presumption of innocence and electronic evidence (Chapters 2 to 4), with a deeper analysis of its handling and admissibility in criminal proceedings, which includes a more detailed analysis of scientific and practical problems (Chapter 6).

In conclusion, I believe that the authors bave successfully fulfilled the set goal and created a handbook that will help primarily practitioners, but also anyone interested, to understand the specific features of electronic evidence and become familiar with the legai framework that govems their acquisition and use in criminal proceedings, as well as with legal issues and practical problems that arise. The additional value of the Toolkit is that it introduces practitioners in a timely manner to the new E-Evidence Regulation for obtaining e-evidence abroad, which will prepare them for its application in 2026. Also, its special value lies in the fact that the emphasis is placed on the protection of the presumption of innocence and the procedural rights of the defence when acquiring and using electronic evidence. The Toolkit will therefore be very useful for defence lawyers, whose training is often neglected when adopting new EU legislation. With ali this in mind, the Toolkit will be a valuable contribution in this area, and I therefore recommend its publication.

In Zagreb, 26 May 2024

Dr Marin Bonačić,
Associate Professor,
Head of Department of Criminal Procedure
at University of Zagreb, Faculty of Law


ANNALES
ZRS

ISBN 978-961-7195-42-02