JUST-2021-JACC

Action grants to support transnational projects
to enhance the rights of persons suspected
or accused of crime and the rights of victims of crime

JUSTICE PROGRAMME

GA No. 101056685

Improving the application of the presumption of iNNOCENce when applying elecTronic evidence

INNOCENT

WP2: Comparative Analysis of Data

D2.1 INNOCENT Report

WP2 leader: Adam Mickiewicz University Poznań

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.

Acronym	**INNOCENT**
Title	Improving the application of the presumption of iNNOCENce when applying elecTronic evidence
Coordinator	Law and Internet Foundation
GA No.	101056685
Programme	Justice Programme (JUST)
Topic	JUST-2021-JACC
Start	16 May 2022
Duration	24 months
Consortium	Law and Internet Foundation (LIF), Bulgaria Adam Mickiewicz University Poznań (AMU), Poland Human Rights House Zagreb (HRHZ), Croatia Bratislava Policy Institute (BPI), Slovakia CEELI Institute (CEELI), Czechia Science and Research Centre of Koper (ZRS), Slovenia

Dissemination level		
PU	Public	X
SEN	Sensitive, limited under the conditions of the Grant Agreement	
EU - R	RESTREINT-UE/EU-RESTRICTED under Decision 2015/444.	
EU - C	CONFIDENTIEL-UE/EU-CONFIDENTIAL under Decision 2015/444	
EU - S	SECRET-UE/EU-SECRET under Decision 2015/444	

Document version control:		
	Author(s)	**Date**
Version 1	Drafted by: Karolina Kiejnich-Kruk, **AMU**	01/10/2022
Version 2	Reviewed by: Martyna Kusak, **AMU**	02/10/2022
Version 2	Updated by: Karolina Kiejnich-Kruk, **AMU**	04/10/2022
Version 2	Reviewed by: Snezhana Krumova, **LIF**	06/10/2022
Version 3	Updated by: Karolina Kiejnich-Kruk, **AMU**	16/10/2022
Version 3	Reviewed by: Snezhana Krumova, **LIF**	17/10/2022
Version 4	Updated by: Karolina Kiejnich-Kruk, **AMU**	21/10/2022
Version 4	Reviewed by: **HRZR**	02/11/2022
Version 4	Reviewed by: **BPI**	03/11/2022
Version 4	Final review and update by: **LIF**	14/11/2022

Table of contents

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.

Abbreviations

Abbreviations	Descriptions
Art.	Article
CoE	Council of Europe
DF	Digital Forensic
e-evidence	electronic evidence
ECHR	European Court of Human Rights
EIO	European Investigation Order
EPO	European Preservation Order
EU	European Union
incl.	including
LEA	law enforcement agency
MS	Member State
PINs	personal identification numbers
PSACs	people suspected or accused of crimes
the Cybercrime Convention	The Convention on Cybercrime, opened for signature in Budapest, Hungary, in November 2001
WP	Work Package

Glossary

Terms	Description
Access data*	'*Data related to the commencement and termination of a user access session to a service, which are strictly necessary for the sole purpose of identifying the user of the service (date and time of use, log-in to and log-off from the service, IP address, user ID)*'.
Burden of proof	'*A legal standard that requires parties to demonstrate that a claim is valid or invalid based on facts and evidence presented. Burden of proof is typically required of one party in a claim, and in many cases, the party that is filing a claim is the party that must demonstrate that the claim is valid and carry the burden of proof.*'
Content data*	'*Any stored data in a digital format such as text, voice, videos, images, and sound other than subscriber, access or transactional data*'.
Digital chain of custody	'*Digital chain of custody is the record of preservation of digital evidence from collection to presentation in the court of law. This is an essential part of digital investigation process. Its key objective is to ensure that the electronic evidence presented to the court remains as originally collected, without tampering. The chain of custody is important for admissible evidence in court. Without a chain of custody, the opposing attorney can challenge or dismiss the evidence presented.*'

Digital forensics	*'…a branch of forensic science that focuses on identifying, acquiring, processing, analysing, and reporting on data stored electronically…The main goal of digital forensics is to extract data from the electronic evidence, process it into actionable intelligence and present the findings for prosecution. All processes utilise sound forensic techniques to ensure the findings are admissible in court.'*
Electronic evidence (e-evidence) *Rationale – wider used than "digital evidence" and within the majority of EU relevant documents*	*'Any data that can serve as evidence, regardless of whether it is stored on or generated, processed or transmitted by an electronic device. It includes both 'content data', such as e-mails, text messages or photographs, and 'non-content data', such as subscriber and traffic data (e.g. the routing or timing of a message)'*
Fair trial	*As prescribed by Article 6 of the European Convention on Human Rights (ECHR)*
Internet service provider (ISP)	'A *company that provides Internet connections and services to individuals and organisations. ISPs may also provide software packages (such as browsers), e-mail accounts, and a personal website or home page. ISPs can host websites for businesses and can also build the websites themselves. ISPs are all connected to each other through network access points, public network facilities on the Internet backbone*'.
Metadata	*'Refers to electronic information about other electronic data, which may reveal the identification, origin or history of the evidence, as well as relevant dates and times'.*

Mutual Legal Assistance Treaties (MLAT)	*MLATs can be either multilateral or bilateral agreements for cooperation between states for obtaining assistance in the investigation or prosecution of criminal offences. For instance, gathering and exchanging information, including obtaining e-evidence. Such requests are made by a formal international Letter of Request. Such assistance is usually requested by courts or prosecutors and is also referred to as 'judicial cooperation'. It is usually a long and complex process. There are foreseen procedures for emergency requests under specific circumstances.*
Subscriber data*	*'Any data pertaining to: a) the identity of a subscriber or customer such as the provided name, date of birth, postal or geographical address, billing and payment data, telephone, or email; b) the type of service and its duration'.*
Transactional data*	'*Data related to the provision of a service offered by a service provider that serve to provide context or additional information about such service and are generated or processed by an information system of the service provider (e.g. metadata, location data)*'.
Trust service	A*n electronic service normally provided for remuneration which consists of:* *(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or* *(b) the creation, verification and validation of certificates for website authentication; or* (c) *the preservation of electronic signatures, seals or certificates related to those services*;'.
Trust service provider	'*A natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provide*'.

* All categories of data above with (*) contain personal data and thus the relevant EU data protection *acquis* should be taken into account.

Introduction

This report is a deliverable D2.1 of Work Package 2 (WP2) "Comparative Analysis of Data" of the INNOCENT project "Improving the application of the presumption of iNNOCENce when applying elecTronic evidence" funded by the European Commission under the JUST Programme.

The project, started in May 2022, focuses on procedural rights of persons suspected or accused of crime, in particular on the right to be presumed innocent until proven guilty, and how it should be understood in context of applying electronic evidence. INNOCENT targets exclusively Central and Eastern Europe in order to map the similarities, best and worst practices in the region with regards to the practical application of the presumption of innocence. It further aims to enhance the cooperation between these neighbouring jurisdictions in regard to the juncture between the presumption of innocence and electronic evidence. The planned activities consist of co-creating training materials, capacity-building events, and policy guidelines and recommendations. The target groups are judges, including investigative judges, prosecutors, defence lawyers, including legal aid practitioners. They will benefit from the project activities by improving the performance of their duties in more reliable, scientifically proven and transparent manner as well as the performance rate in terms of investigation practices.

In this context, T2.1. coordinated by Adam Mickiewicz University Poznan (AMU) aims to carry out secondary research and identify already existing knowledge, generated under research in the same field already done under previously EU funded projects, as well as literature, reports and legal framework existing in the same area of interest. The task is narrowed to the period of 2010-2022 for consistency purpose with the case law review under T2.2.

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.

1. Aim of the study

The study under this task -2.1 Overview of existing practices and expanding of previous research - aims to examine what has already been established about the impact of electronic evidence on the presumption of innocence and what areas need further examination or amendments, and during further project works, how this can be turned into know-how for practitioners.

This document presents an overview of existing practices and knowledge and recognises the areas of previous research that should be expanded and examined. This will help to:

a) set the scene for the project and identify the fields to be expanded and further explored,

b) outline questions to be included in the template under the further task such as co-creation meetings,

c) avoid double work and double funding.

2. Methodology and the structure of the report

The research conducted under T2.1. uses desktop research methodology (secondary research method). It enables to use existing data to set a floor to the proper research and determine its scope as well as to pose relevant questions and research areas before the co-creation meetings and workshops. It is a cost-effective way to obtain relevant data from a broad range of sources. Relevant EU funded projects has been recognised with the use of CORDIS database. All the information about EU funded projects come from the projects' websites and their deliverables. Literature review has been done with the use of the open-access sources. Key words used to search were: *electronic evidence, e-evidence, digital evidence, presumption of evidence*.

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.

Regarding legal frameworks, a legal analysis method has been used, including the use of access to the EU legal acts via EUR-lex.[1]

The research has been narrowed to the studies done within the period of 2010-2022.

The structure of the report is as follows:

1. in the first part (point 5.1.) EU funded projects are presented, from the most to the least relevant for INNOCENT,
2. the second part (5.2.) is divided into three subsections: legal frameworks, policy papers and legislation related research and finally literature review studies,
3. the third and fourth parts (5.3. and 5.4.) presents the study results narrowed to two main areas of interests regarding the report - the fields to be further explored during INNOCENT and these still unexplored,
4. finally, point 6. shows the conclusions of the study.

3. The state of art

3.1. EU funded projects

Among the EU-founded project none directly relates to electronic evidence in the context of presumption of innocence. However, some fields tackling these issues have been already explored within previous research and projects. What seems to be particularly relevant for the INNOCENT project, is the area of handling of electronic evidence during its entire lifecycle (the acquisition and collection, decryption, analysis, preservation, admissibility, use and exchange of electronic evidence). As the part of it, there is an issue of the harmonisation of these standards among EU countries. Equally relevant are the results of the projects that tackled the problem of the protection of the fundamental rights across the EU while applying electronic evidence or other technological solutions.

Respective EU funded projects and their results - significant for INNOCENT - are presented below.

[1] Access to European Union Law, https://eur-lex.europa.eu (access: 13.10.2022).

1. **EVIDENCE project** („European Informatics Data Exchange Framework for Courts and Evidence"[2]) examined many aspects of the problems presented above. Although its main interest was the exchange of e-evidence between EU Member States (MS), many outcomes and results can be considered as relevant for INNOCENT.

EVIDENCE provides an overview of practices and procedures for digital evidence gathering, concerning tools that are thoroughly tested and generally accepted in the computer forensics field in the MS as well as an overview of existing standard for treatment and exchange of electronic evidence. One of the results of the project is the tools checklist whereby all the authorised people check the available tools and their appropriateness regarding the investigation to be carried out and the guidelines to follow specific standard procedures, based on the kind of device to be handled.[3] **Existing digital evidence processing systems are mapped, described and classified according to the technology/method used and the purposes for which they were originally designed or actually used. This tool can be useful for practitioners: judges, prosecutors, LEAs in daily basis procedural actions.** It can set a base for the future INNOCENT activities such as workshops or meetings, when the technical knowledge gathered under WP4 of EVIDENCE can be used.

Within the project, a set of best practices and guidelines for mobile devices have been defined. The followed the source considered as the most authoritative one, which is the "NIST Guidelines on Mobile Device Forensics" (the last version of which was issued in May 2014).[4] The guide describes all the activities to be carried out on the basis of the state of mobile device, subject to seizure. The distinction to the two different situations had been made: when the device is switched off or left on.

The research tackled the problem of the access to the personal devices, however not in the aspect of possible infringement of the presumption of innocent and forcing suspects

[2] European Informatics Data Exchange Framework for Courts and Evidence project, http://www.evidenceproject.eu (access: 13.10.2022).
[3] Deliverable D4.1, http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d4-1-413.pdf (access: 13.10.2022).
[4] NIST Guidelines on Mobile Device Forensics, https://www.nist.gov/publications/guidelines-mobile-device-forensics (access: 13.10.2022).

or accused to convey the passwords or fingerprints to unblock the devices. As an outcome of the research, it has been emphasised that the legal framework for online investigations, electronic evidence and mutual legal assistance severely lags behind everyday reality and no longer provides a solid basis for law enforcement, forensic institutes and lawyers to fulfil their proper roles.

Following gaps have been detected:

a) need for a common and shared understanding on electronic evidence,
b) need for a common European Legal Scenario on electronic evidence,
c) need for a Common perception and reliability on electronic evidence for stakeholders,
d) need for rules and standardised procedures for Exchanging digital evidence.

EVIDENCE tackled the problem of authenticity of evidence, but it was not the area of main interest. However, it has been suggested and proposed that cloud space is the right move to store and preserve metadata as a safe space to avoid any data modifications. However, the risk of that has been also emphasised.[5] What can be further examined is the answer to the question: what metadata should be preserved to be able to check the authenticity of the evidence and avoid any possibilities of the modifications.[6] Such actions could help to protect the presumption of innocence rules and avoid using false or manipulated evidence in criminal proceedings.

Main result of the **EVIDENCE** project is a 'Roadmap'.[7] 'Roadmap' is meant to be a resource for legislators, policymakers, LEAs and any other stakeholders with an interest in electronic evidence and is meant 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 core findings of the EVIDENCE project are that:

---

[5] Workshop on Categorization 'Semantic Structure of Electronic Evidence', http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d11-3-429.pdf (access: 13.10.2022).
[6] Ibidem.
[7] Deliverable D9.2., http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d9-2-426.pdf (access: 13.10.2022).

1) there is no comprehensive legal framework as regards electronic evidence collection, preservation, storage, use and exchange,
2) in spite of this lack of comprehensive legal framework electronic evidence is increasingly key evidence in criminal procedures,
3) the lack of this comprehensive legal framework leaves LEAs to operate in a patchwork of solutions, be it legal, data protection, enforcement or technical solutions,
4) the stakeholders involved 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.

As regards competences and professions, it has been detected that there is a lack of technical knowledge, experience and training within the judiciary as well as with prosecution and defence lawyers. It is a challenge to stay up to date with all the innovations and tools. Investing in proper digital forensic tools is 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.

According to the authors of the report, it is desirable that every judicial actor is trained to guarantee minimum knowledge on electronic data and its use in the judicial system in order to reduce the waste of time and resources and to increase trust. This needs to be addressed by mandatory training (on technical issues/ electronic evidence/ digital forensics) of the judiciary in the field of electronic evidence. Coordinated European training programmes should be set up and carried out within the MS in order to train judiciary officials within the field of electronic evidence. It is furthermore advisable to compile more information on the subject matter and develop a (cyber)crime repository including a repository of case law and lessons learnt.

EVIDENCE diagnosed main obstacles regarding collecting, preserving, using, exchanging e-evidence. These are:[8]

[8] Deliverable D7.2. and D7.3., http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d7-2-420.pdf and http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d7-3-421.pdf (access: 13.10.2022).

A. Mistrust of the judicial authorities regarding electronic evidence

B. **Issues relating to competences and professions (including operators lacking experience, lack of training courses, lack of specific competences in the local police, difficulties in presenting evidence at court in a way that is comprehensible, few experts, vagueness of digital forensic profession)**

C. Security issues

D. Fragmentation

E. **Cultural and personal opposition (including difficulties in following technological changes in the field of electronic evidence, failure to take into account the specificity of electronic evidence)**

F. Isolation of the technological process

G. **Lack of governance (incl.: lack of specialised judicial services, assignment of cases to judges who are not experts in the field, difficulties in the relation between law enforcement agencies and international server providers, difficulties related to the non-binding nature of international cooperation in this area, difficulties due to lack of jurisdiction)**

H. **Difficulties of a functional nature (incl.: lack of procedures or guidelines for obtaining, preserving and presenting electronic evidence, overwhelming quantity of data requiring analysis)**

as well as facilitating factors:

A. Creation of a favourable technological and professional environment

B. Promotion of the introduction and management of electronic evidence

C. Support policies.

Among others, the **EVIDENCE** project outcomes are:[9]

1) as proof of the extent to which electronic evidence is less willingly accepted at court, it was observed that in many cases judges are mistrustful and ask for more guarantees than with other kinds of evidence (Source: EVIDENCE, 2013 - but in EVIDENCE 2015 this approach has NOT been VALIDATED/CONFIRMED),

[9] Deliverable D7.2., http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d7-2-420.pdf (access: 13.10.2022).

2) **one of the reasons why judges and prosecutors often reject electronic evidence in trials is that they do not understand the nature and characteristics of this kind of evidence very well,**
3) **many working in the legal profession (judges, lawyers, etc.) have not received adequate training in the management of electronic evidence (for example, prosecutors were found to lack computer skills),**
4) there is a widespread shortage of courses that offer structured, continuous and certified training in the field of electronic evidence management,
5) the shortage or lack of specialised judicial services is a serious impediment to the speed and effectiveness of electronic evidence collection and management.

INNOCENT project aimed at organising training sessions and workshops and in that way answers the needs that has been indicated in **EVIDENCE** conclusions.

2. The **FORMOBILE** project („From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices")[10] provides with technical knowledge about mobile devices and acquiring electronic evidence from them.

FORMOBILE project, as the **EVIDENCE** project, touched the problem of the cloud storage. As it has been indicated, „data acquisition from the cloud is highly challenging since there are so many providers. Many of the technological, organisational, and legal problems related to retrieving this data are still unsolved".[11] That shows the technical background, distinctions of the cloud storage, different models, and again – can be used as a base of the professional knowledge during workshops addressed to LEAs and court on the subjects concerning how to proceed with this kind of data.

„File Format Handbook" – **FORMOBILE** result – summarises knowledge about various file formats and file systems common in mobile devices. According to the Authors, this book is not only a toolbox for the investigators having a deep knowledge about digital investigations from real cases. The book is also aimed at people who are new to digital

[10] From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices, https://formobile-project.eu/project (access: 13.10.2022).
[11] D. Pawlaszczyk, M. Bochmann, P. Engler et al., *API-based evidence acquisition in the cloud - a survey [version 1; peer review: 1 approved with reservations],* Open Res Europe 2022, 2:69, https://doi.org/10.12688/openreseurope.14784.1 (access: 13.10.2022).

forensics and are interested in the general theory of file recovery and file systems.. Part I describes several different file systems that are commonly used in mobile devices. Part II describes five different file formats that are commonly used on mobile devices.[12]

Some information regarding recovering delated data is presented in the article „Making the Invisible Visible – Techniques for Recovering Deleted SQLite Data Records" (part of **FORMOBILE**).[13]

„Guidance Document"[14] (**FORMOBILE**) should enable legal practitioners to create a Checklist Guidance Document in order to determine the inevitable actions that have to be done and must not be done. The actions can be applied in the specific proceedings of a given case to **guarantee the admissibility, relevance and probative value of digital evidence derived from mobile devices**. The Checklist Guidance Document enables legal practitioners - in particular criminal judges - 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 a court.

The document provides us 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 the practitioners to assess the data gained from electronic devices. It also sets **the roles of the main actors and their goals during criminal proceeding involving e-evidence** (particularly ones extracted from mobile devices)**,** what is particularly important when looking for the ones that should be supporting the protection of the fundamental rights of accused and suspects, especially the presumption of innocence.

FORMOBILE prepared several courses on the subject of electronic evidence, computer science technologies and techniques, mobile devices, addressed to judges, prosecutors,

---

[12] *Mobile Forensics – The File Format Handbook. Common File Formats and File Systems Used in Mobile Devices*, ed. Ch. Hummert, D. Pawlaszczyk, https://link.springer.com/content/pdf/10.1007/978-3-030-98467-0.pdf (access: 13.10.2022).

[13] D. Pawlaszczyk, *Making the Invisible Visible – Techniques for Recovering Deleted SQLite Data Records*, International Journal of Cyber Forensics and Advanced Threat Investigations 2021, 1:1, https://www.researchgate.net/publication/348834288_Making_the_Invisible_Visible_-_Techniques_for_Recovering_Deleted_SQLite_Data_Records (access: 13.10.2022).

[14] Guidance to Checklist Preparation for Legal Practitioners, https://formobile-project.eu/downloads/publications-public-deliverables/157-formobile-legal-checklist-guidance-document-final/file (access: 13.10.2022).

LEAs. The overarching objective of **FORMOBILE** was to establish a complete end to end forensic investigation chain, targeting mobile devices. In general, **FORMOBILE** provides a technical view on the issue of electronic evidence gathered from mobile devices and shape a base for the further research and activities, such as workshops and meetings.

Both EVIDENCE and FORMOBILE stress the need for the trainings, workshops, courses and all the tools aimed at raising knowledge and awareness of the practitioners on the subject of the e-evidence and new technologies.

3. As regards to the electronic evidence, **LIVE-FOR**[15] project is also relevant. The project collected and analysed information about the status of implementation of the Directive on the European investigation order in EU Member States, digital evidence related practices, best practices, and educational needs by means of surveys, face-to-face meetings with target groups and various analytical methods. B. Blažič and T. Klobučar[16] (as a result paper of the project) examined EIO in the context of the electronic evidence and stated that the usefulness of the EIO in cybercrime cases that involved e-evidence was not confirmed. Analysing the results of the experts' meetings during the project, they stated that „the need for effective (cross-border) remote e-evidence searches as well as for unilateral preparations of the data requests to foreign service providers and other providers acting in the EU Member State". **EIO did not seem sufficient when it comes to cross border e-evidence actions in criminal proceedings.** Turning to future EPOs instruments, it has been emphasized that EU bodies envisage the training of public authorities in cooperation with US-based providers to support the functioning of the direct cooperation between both. Such trainings are desirable and seem to be crucial for the success of the projected instruments[17].

4. Regarding presumption of innocence issue, one of the most recent studies conducted in the Central and Eastern Europe focused on the presumption of innocence in the context of the media and public in Croatia and how suspects and accused are presented

[15] LIVE_FOR, http://live-for.eu (access: 13.10.2022).
[16] B. Blažič, T. Klobučar, *Investigating crime in an interconnected society: will the new and updated EU judicial environment remove the barriers to justice?*, International Review of Law, Computers & Technology 2020, 34:1, pp. 95-96.
[17] Ibidem, p. 103.

(„**The importance of appearances: how suspects and accused persons are presented in public and in the media**").[18] What seems to be a rule is that despite of exciting ethical and legal frames, media do not obey the requirements. What seems to be a standard is to present suspects or accused as an offender (a murderer/killer, a smuggler, a hijacker). Such presentation has an impact on the perception of the suspect or accused. It is very important to count such practices.

5. The aim of the project **PRESENT** („Enhancing the Right to be Present PRESENT")[19] is to enhance the right to be present at trial for persons suspected or accused of crimes, as well as to strengthen certain aspects of the presumption of innocence.

The project provides us with the Recommendation List[20] that contains all measures, which have been identified to be most successful and effective regarding the implementation and application of Directive 2016/343[21] and that could be applied in all countries participating in the project **PRESENT**. The recommendations on the amendments that could be made in all of the countries regarding implementation of the Directive 2016/343 are relevant, however they are focused on the right to be present more than the presumption of innocence.

One of the project outcomes is **a comparative analysis of how and to what extent the Directive has been transposed in the six partnering Member States. It highlights areas of success in implementing the minimum procedural safeguards but also disclose the failures and gaps in complying with the Directive.** The objective is to

[18] The importance of appearances: how suspects and accused persons are presented in public and in the media, https://www.kucaljudskihprava.hr/wp-content/uploads/2019/06/Media_report_SIR_eng.pdf (access: 13.10.2022).
[19] Enhancing the Right to bePresent PRESENT, https://www.netlaw.bg/en/a/enhancing-the-right-to-be-present-present (access: 13.10.2022).
[20] Deliverable D3.4, https://www.netlaw.bg/p/r/e/recommendation-list-2467.pdf (access: 13.10.2022).
[21] 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.

underline best practices, if possible, in the different areas provided for by the Directive in following MS: Bulgaria, Romania, Cyprus, Slovakia, Portugal, Austria.[22]

The project resulted in a paper that presents a brief overview of the legislative *status quo* in Bulgaria concerning the use of information and communication technologies in the area of criminal proceedings.[23] What is particularly relevant is the concept of the e-Justice system. The aim of the concept is to achieve **the same level of effectiveness of procedural rights exercise in electronic form as the one currently attached to procedural rights exercised in the paper-based environment** by amending the current legislation. Thus, the national concept for electronic justice aims to ensure that procedural rights are equally protected in electronic and paper-based format.

It is clear that use of electronic evidence and electronic justice systems are not directly linked. However, **experiences gained while implementation electronic justice systems, issues pertaining the protection of fundamental rights can be useful and can set an example for the implementation of the electronic evidence rules in courts.**[24]

6. Under the **FAIR** project („Enhancing the Fair Trial for People Suspected or Accused of Crimes")[25] deep research concerning the state of implementation of the Directive (EU) 2016/343[26] in MS has been conducted. One of the outcomes of the project is the report showing on the example of the 4 countries legislature how the MS implemented the

[22] C. Paraskeva, N. Hatzimihail, E. Meleagrou, *General Report: Comparative Analysis of the Legal Treatment of the Right to be Present and the Presumption of Innocence in the PRESENT partner States in the light of Directive 2016/343*, http://www.lex-localis.press/index.php/LexLocalisPress/catalog/book/68 (access: 13.10.2022).

[23] D. Kozhuharova, A. Kirov, *What lies ahead in the future for the Information and Communication Technologies' Use in the Criminal Procedure?*, http://www.lex-localis.press/index.php/LexLocalisPress/catalog/book/68 (access: 13.10.2022).

[24] Bulgaria can set an example. The country represents the trend that can be detected in the most of the EU MS. The BCPC does not explicitly regulate e-evidence. It can be easily seen that despite implementing packages of the new technologies regulations, e-justice systems, do not implement any regulation addressing use of electronic evidence.

[25] Enhancing the Fair Trial for People Suspected or Accused of Crimes, https://www.netlaw.bg/en/a/enhancing-the-fair-trial-for-people-suspected-or-accused-of-crimes-fair (access: 13.10.2022).

[26] 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.

Directive to their law system and how the detailed provisioned have been understood and transposed in practice.[27] On this example it can be recognised that not all the provisions have been fully implemented or properly implemented, what be important for INNOCENT.

The Data Collection report[28] (**FAIR** Deliverable) presents a comparative analysis of the findings regarding the actual implementation of the Directive (EU) 2016/343 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings. The studies in the countries involved in project (Austria, Bulgaria, Hungary and Greece) shows that **there are cases where LEAs and judges circumvent the presumption of innocence rule**, mostly by taking advantage of the absence of lawyer on the earliest parts of the proceedings and strongly encouraging or forcing by threat or promise to cooperate with LEAs. The case law studies has not been focused on the acquiring e-evidence, however **such tendency of the misbehaviour should be a warning that the similar situations can occur regarding possessing e-evidence, passwords to electronic devices, accessing these devices in any other way.**

Stakeholders in each of the countries mentioned a number of good practices that have strengthened the presumption of innocence. However, it should be noted that the majority of the mentioned good practices constitute either legal requirements (Austria, Bulgaria and Hungary) or aspirations regarding the implementation of the presumption of innocence (Greece). **The role of the defence lawyer from the early stage was strongly emphasised as the guarantee of the presumption of innocence.**[29]

---

[27] Deliverable D2.3, https://www.netlaw.bg/en/a/enhancing-the-fair-trial-for-people-suspected-or-accused-of-crimes-fair (access: 13.10.2022).

[28] Deliverable D.2.2., https://www.netlaw.bg/en/a/enhancing-the-fair-trial-for-people-suspected-or-accused-of-crimes-fair (access: 13.10.2022).

[29] Deliverable D2.2., https://www.netlaw.bg/en/a/enhancing-the-fair-trial-for-people-suspected-or-accused-of-crimes-fair (access: 13.10.2022); there are various approaches followed by the countries when it comes to the suspects or accused right to remain silent and the right to not incriminate against themselves in criminal proceedings. A common finding (Bulgaria and Hungary) highlights the pressure that might be exercised on PSACs suggesting them to confess or agree to testify in order to be helped by the authorities. Another finding (Austria and Greece) that could be considered as common is that the right to remain silent is poorly communicated in practice (hence,

The **FAIR** Best Practice Handbook[30] is aimed at providing selected criminal justice practitioners, particularly police officers, prosecutors, judges and lawyers with recommendations for their daily work in order to enhance the fair trial for people suspected or accused of crimes. Moreover, the current handbook includes precise and up-to-date knowledge about the implementation of six EU Directives (procedural roadmap) in Austria, Bulgaria, Greece and Hungary, as well as about the practical challenges for the authorities and people suspected or accused of crimes (PSACs) alike.

7. **ProCam** („Procedural Rights Observed by the Camera")[31] project examines the connection between the audio-visual recording of any questioning of vulnerable persons and the enforcement of their rights, examining the role of audio-visual recording in securing the rights granted in Directive 2013/48, analysis of the international standards, comparison of the Member State laws and practices, reform proposal aimed at reinforcing good practices, researching practices in the 28 EU Member States Procedural rights observed by the Camera.[32] The country report shows that main obstacles regarding the audio-visual recording are the technical and technological problems and preserving of the recordings and delivering them to the court. **It has been seen that the implementation of the ‚Roadmap' directives in the MS has not been fully successful what seems to be the universal problem for both - all MS and all directives.** The problem of the forced testimonies has been also emphasised. In some MS bad practices exist, such as forcing PSACs to testify, especially during the first interrogation and in the absence of defence lawyers. Obligation of audio-visual recording could help in countering such misbehaviour as well as violating the presumption of innocence (e.g. forcing PSACs to reveal passwords, give fingerprints to access mobile devices etc.).

---

in Greece PSACs do not make use of this right out of fear that it will have a negative impact on their case).

[30] Deliverable D2.4., https://www.netlaw.bg/en/a/enhancing-the-fair-trial-for-people-suspected-or-accused-of-crimes-fair (access: 13.10.2022).

[31] Procedural Rights Observed by the Camera, https://www.oijj.org/en/our-work/research/projects/procam-procedural-rights-observed-camera-audiovisual-recordings (access: 13.10.2022).

[32] Audiovisual recording of interrogations in the EU (2018-2019) (ProCam), Comparative Report, https://www.antigone.it/upload2/uploads/docs/ProCamcountryreportIT.pdf (access: 13.10.2022).

8. 'Report on data protection and other fundamental rights issues'[33] (one of the **EVIDENCE2e-CODEX**[34] deliverables) examines how data protection implications in European Investigation Orders and Mutual Legal Assistance procedures are being handled. The report examines how data protection implications are being handled and identifies legal and/or operational measures that need to be put in place to ensure respect to data protection rights especially in the case of electronic evidence. In one word, it shows the *status quo* of these issues.[35]

As the new technologies develop rapidly, there are some projects aimed at innovative measures to acquire data and information that are used as the electronic evidence in the courtroom. Particularly relevant - regarding criminal proceedings - are:

9. **ROXANNE** („Real time network, text, and speaker analytics for combating organised crime")[36] aimed at combining new speech technologies, face recognition and network analysis to facilitate the identification of criminals and developing a platform that will increase agencies' capabilities via voice recognition, language and video technologies,

10. **FORENSOR** („FOREnsic evidence gathering autonomous seNSOR")[37] aimed at inventing new methods of the evidence gathering (considering new technologies) and developing and validating a novel, ultra-low-power, intelligent, miniaturised, low-cost, wireless, autonomous sensor ("FORENSOR") for evidence gathering (ultra-sensitive camera and built-in intelligence will allow it 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),

---

[33] Deliverable D2.3, https://evidence2e-codex.eu/p/e/v/evidence2e-codex-deliverable-d2-3-summary-436.pdf (access: 13.10.2022).
[34] EVIDENCE2e-CODEX, https://evidence2e-codex.eu (access: 13.10.2022).
[35] Deliverable D2.3. https://evidence2e-codex.eu/p/e/v/evidence2e-codex-deliverable-d2-3-summary-436.pdf (access: 13.10.2022); The final part of the report examines where fundamental rights, other than the right to the protection of personal data, are directly or implicitly referred to in the EIO Directive, and how they are being handled in a selection of different Member States.
[36] Real time network, text, and speaker analytics for combating organised crime, https://roxanne-euproject.org (access: 13.10.2022).
[37] FOREnsic evidence gathering autonomous seNSOR, https://cordis.europa.eu/project/id/653355 (access: 13.10.2022).

11. **TITANIUM** („Tools for the Investigation of Transactions in Underground Markets")[38] - developing novel methods and technical solutions for investigating and mitigating illegitimate activities involving virtual currencies and/or underground market transactions and providing low-cost and open-source tools for cryptocurrency forensics,

12. **3D-FORENSICS** („Mobile high-resolution 3D-Scanner and 3D data analysis for forensic evidence")[39] - analysing the forensic evidence, developing accurate system - 3D-reconstruction of evidence and its analysis (e.g.: for footwear and tyre impression traces).

The **ROXANNE** project will support LEA's activities through multilanguage applications based on voice, text and face technologies. ROXANNE, in conformity with Interpol and EU regulations, will be tested on real case data in nine EU Member States. The „Initial speech/text/video technologies" report[40] summarises mentioned technologies available at the outset of the project. It first gives a non-expert overview of such technologies and concentrates on their use in LEA framework.[41]

FORENSOR proposes to develop and validate a novel, ultra-low-power, intelligent, miniaturised, low-cost, wireless, autonomous sensor ("FORENSOR") for evidence gathering. Its ultra-sensitive camera and built-in intelligence will allow it 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. FORENSOR will be able to operate for up to two months with no additional infrastructure. It will be manageable remotely, preserve the availability and the integrity of the collected evidence, and comply with all legal and ethical standards, in particular those related to

[38] Tools for the Investigation of Transactions in Underground Markets, https://www.titanium-project.eu (access: 13.10.2022).
[39] Mobile high-resolution 3D-Scanner and 3D data analysis for forensic evidence, https://cordis.europa.eu/project/id/312307 (access: 13.10.2022).
[40] Deliverable D5.1., https://roxanne-euproject.org/results/files/d5-1.pdf (access: 13.10.2022).
[41] Real time network, text, and speaker analytics for combating organised crime, https://roxanne-euproject.org (access: 13.10.2022).

privacy and personal data protection. The combination of built-in intelligence with ultra-low power consumption could help LEAs take the next step in fighting severe crimes.[42]

The EU-funded **TITANIUM** project is providing European law enforcement agencies with the tools they need to identify cybercriminals – even when they operate behind the pseudo-anonymity of virtual currencies. The TITANIUM Toolset provides improved investigation capabilities for LEAs in virtual currency and darknet market analytics compared to simple methods presently used by many investigators. These low-cost and open-source tools developed in the context of TITANIUM can compete with commercial tools in terms of total costs of ownership, and can therefore be provided to more investigators, leading to improved capabilities, more rapid and less expensive investigations for Europe as a whole. The Authors tackled the problem of the protection of fundamental rights.[43] The processing of personal data can constitute an interference with fundamental rights. Of particular relevance for TITANIUM are the right to data protection and the right to protection of private life which are constituted on European level. As it was indicated in the conclusions, for judicial/legal review a comprehensive assessment of all tools actually used in the investigation is necessary. The lower the interference of each individual tool, the lower the overall interference with fundamental rights to data protection and privacy. The report contains proposals and rules that has been set to avoid infringements or discrimination and principles of data protection law i.e., purpose limitation, data anonymisation.[44]

Outcomes of the projects are relevant for INNOCENT due to their high potential in developing tools for obtaining electronic evidence later used in criminal proceedings. **Increasing the efficiency of LEAs in acquiring e-evidence is the one thing, but another one is to create safeguards that are able to protect the fundamental rights while using these tools and their fruits in courts.**

---

[42] FOREnsic evidence gathering autonomous seNSOR, https://cordis.europa.eu/project/id/653355 (access: 13.10.2022).

[43] Deliverable D2.1., https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c8a88508&appId=PPGMS (access: 13.10.2022).

[44] Tools for the Investigation of Transactions in Underground Markets, https://www.titanium-project.eu (access: 13.10.2022).

13. There is also a research project „**Admissibility of E-Evidence in Criminal Proceedings in the EU**"[45] conducted by the European Law Institute between the date: September 2020–December 2022. According to the website, „the project will develop **a legislative proposal on admissibility and exclusionary rules of e-evidence in criminal proceedings**, which will be accompanied by a background study analysing (1) general principles on admissibility/exclusion of criminal evidence, taking into account different national approaches of selected EU Member States; (2) relevant case law of the European Court of Human Rights; (3) the protection of the lawyer-client privilege in digital searches and the cross-border impact of such searches and (4) the identification of immunities that should be protected and whether the protection should be the same as with regard to the lawyer-client confidentiality relationship"[46], however no results have been published so far.

3.2. Legal framework and literature review

3.2.1. Legal framework

As regards to legal framework and policy documents pertaining electronic evidence and presumption of innocence, both EU and CoE systems must be considered. The latter states the frame for the Cybercrime Convention[47] and its Second Protocol.[48] The EU law only serves the purpose of exchanging evidence across borders. So did the CoE's law, but the provisions of the Cybercrime Convention required some action to implement specific provisions in national law. According to the Cybercrime Convention's provision, each country is obliged to adopt legislative and other measures that may be necessary to preserve stored computer data (Art. 16), order to submit necessary data (Art. 18), search and seizure of stored computer data (Art. 19), collect real-time traffic data (Art. 20), intercept of content data (Art. 21). **The Cybercrime Convention obliges the countries**

[45] Admissibility of E-Evidence in Criminal Proceedings in the EU, https://www.europeanlawinstitute.eu/projects-publications/current-projects/current-projects/admissibility-of-e-evidence/ (access: 13.10.2022).
[46] Ibidem.
[47] The Convention on Cybercrime, opened for signature in Budapest, Hungary, on November 23, 2001.
[48] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, November 17, 2021.

to subject to conditions and safeguards provided for under its domestic law, protect human rights and liberties, including rights arising pursuant to obligations under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (Art. 15).[49] The ECHR in Article 6 (2) references directly to the presumption of innocence rule and states that everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.

Second Additional Protocol to the Convention on Cybercrime[50] on enhanced co-operation and disclosure of electronic evidence has been adopted on 17 November 2021. It has been emphasised in the Preamble that MSs of CoE are aware that evidence of any criminal offence is increasingly stored in electronic form on computer systems in foreign, multiple or unknown jurisdictions, and that additional measures are needed to lawfully obtain such evidence. The need for increased and more efficient co-operation between States and the private sector, has been recognised. **The Protocol implements the innovative institution such as direct contact between LEAs and service providers, however regarding subscriber data only (Art. 7).**

The Survey Report on Data retention in the States Parties to the Budapest Convention on Cybercrime shows that it has been noted that surveyed countries need to adhere to „relatively non-harmonised set of conditions under rules of international law".[51] The countries rely on EU law and the ECHR with ECHR case law when it comes to minimum standards of data retention. Outside Europe, International Covenant on Civil and Political Rights[52] seems to be the main human rights instrument but it does not contain any requirements in terms of protecting fundamental rights and freedoms in the context of data retention. It may be important for EU countries regarding the possibility of acquiring evidence from other countries outside of EU. One of the concerns raised by the study's

[49] Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, November 4,1950.
[50] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, November 17, 2021.
[51] Data retention in the States Parties to the Budapest Convention on Cybercrime, Survey report 2020, p. 27, https://rm.coe.int/2088-32-data-retention-report-2020/1680a1f305 (access: 13.10.2022).
[52] International Covenant on Civil and Political Rights, adopted on December 16, 1966.

authors is that the countries should not allow to use retained data in all of the pending proceedings, pertaining to any criminal offence. The line of the EU law and ECtHR's jurisprudence is „to limit application of surveillance to a range of serious offences".[53] It seems that it is also relevant to cross-border evidence from outside of EU.

As regards to EU legal framework, there is no comprehensive rules system regarding electronic evidence. There are only a number of EU instruments which may be directly or indirectly relevant to the collection, preservation, use and exchange of electronic evidence. Two main areas must be considered: 1) European Investigation Order (already in use), 2) European Preservation Order (legislative stage).

Directive 2014/41/EU of The European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters does not specifically refer to electronic evidence. However, due to its wide scope, it constitutes the instrument of first choice for a cross-border exchange of electronic evidence in the EU. What is relevant, in the beginning of 2018, the European Commission launched a consultation procedure in view of the introduction of a Cross-border e-Justice in Europe Regulation, also known as e- CODEX. The system allows the prompt judicial cooperation in cross-border criminal matters. Looking for a link between these tools and regulations and presumption of innocence, it has been detected that **among EU MS there are no common rules or minimum standard** on the systems and techniques on preserving, collecting and storing of electronic evidence, as well as the admissibility of electronic evidence. While honouring the presumption of innocence rule in the criminal proceedings is not always easy when using electronic evidence, it can be envisaged that it would be even more tricky with e-evidence possessed abroad. Access to files and documents data that could facilitate the verification of the e-evidence is even more limited than in internal cases. A clear and more harmonised framework is desirable in order to facilitate efficient cooperation in criminal matters and secure fundamental rights.

[53] Data retention in the States Parties to the Budapest Convention on Cybercrime, Survey report 2020, p. 27, https://rm.coe.int/2088-32-data-retention-report-2020/1680a1f305 (access: 13.10.2022).

In April 2018 the European Commission published 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.[54] Both aimed to establish a new legal regime throughout the EU when it comes to electronic evidence seizure and obtain. The idea behind this initiative is to enable the judicial authorities to directly obtain evidence from a digital services provider without the involvement of public authorities. The legislative package introduces two types of procedures:

1) European Production Order[55] - a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to produce electronic evidence,
2) European Preservation Order[56] - a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to preserve electronic evidence in view of a subsequent request for production.

What is new about the regulation is the scope of the regulation - they are aimed not only to EU service providers, but to all service providers that offer services in EU. Most of them are from United States. Finalising the legislative procedure needs advanced negotiations between EU and US. It is not clear when we can expect coming it into force.

---

[54] 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, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018PC0226&from=EN (access: 13.10.2022); proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF (access: 13.10.2022).

[55] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF (access: 13.10.2022).

[56] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0001.02/DOC_1&format=PDF (access: 13.10.2022).

As regard the principle of presumption of innocence, the EU legal system provides the Directive (EU) 2016/343 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at trial in criminal proceedings. Member States were obliged to ensure that their domestic law was compatible with the Directive and, if necessary, to make all appropriate amendments to their domestic law, by 1 April 2018. As it has been examined within EU funded projects mentioned in this report, it has not been fully succeeded.

3.2.2. Policy documents and legislation-related research

In June 2019, **the Council of European Union adopted conclusion pertaining data retention for the purpose of fighting crime**. The Council recognised that data stemming from telecommunications operators and service providers is essential for the efficiency of criminal proceedings. However, the Council emphasised that „**data retention should be guided by the need to protect fundamental rights**".[57] As a conclusion, the Council invited the Commission to examine the needs of MS judicial authorities and LEAs to have data that are strictly necessary to effectively fight crime, including terrorism. In consequence, we can expect regulation in the EU area pertaining making electronic data (relevant for criminal proceedings) available for competent authorities. It has been detected from the very beginning, that this kind of data regulation has to be in accordance with the Charter of Fundamental Rights of the European Union as interpreted by the Court of Justice.[58]

The report of European Union Agency for Fundamental Rights[59] indicates that „defendants are not obliged to provide evidence incriminating them, for example data

[57] Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime, p. 5, https://data.consilium.europa.eu/doc/document/ST-9663-2019-INIT/en/pdf (access: 12.10.2022); Cybercrime Judicial Monitor, 2019, i. 5, pp. 25-26, https://www.eurojust.europa.eu/sites/default/files/assets/2019_12_cjm_5_en.pdf (access: 12.10.2022).

[58] Conclusions of the Council of the European Union on Retention of Data for the Purpose of Fighting Crime, p. 5, https://data.consilium.europa.eu/doc/document/ST-9663-2019-INIT/en/pdf (access: 12.10.2022).

[59] 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 (access: 12.10.2022).

contained in electronic devices".[60] They do not have any obligation to share data with LEAs, including computer, email passwords, PINs. However, the findings of the report show that such situations occur. T**he LEAs try to encourage them by promise or threat. They can suggest that that kind of cooperation can result in shorter proceedings or milder treatment.** The Authors of the report indicate that „Member States should provide systematic guidance and training to ensure that police officers always explain to defendants their rights, including the consequences of remaining silent, of a confession or of providing evidence or information that incriminates them".[61] Defendants should not be pressured to cooperate and reveal some information, and both threats or promises are not allowed during the hearings.[62]

What is more, regarding incriminating evidence, such as data stored on electronic devices, the majority of interviewees (e.g. professionals from Austria, Germany, Italy and Poland) confirm that defendants are not obliged to provide phone PINs, computer or email passwords or similar information. However, some defence lawyers indicated that, in practice, the LEAs sometimes encourage PSACs to provide incriminating evidence.

What has been detected very often is that „**early access to a defence lawyer as a key safeguard of a defendant's rights**, including to be given adequate information about the rights to remain silent and not to self-incriminate".[63]

Video documenting police interrogations can be a key to the protection of a defendant's right to remain silent if a defence lawyer is not present - in order to avoid any violations of the informing obligation about the right to remain silent.[64]

---

[60] Ibidem, p. … /I cannot open ERA page right now.
[61] Ibidem, p. … /I cannot open ERA page right now.
[62] Ibidem, p. 13.
[63] Ibidem, p. …
[64] Ibidem, 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

Also, **Fair Trials** conduct research connected with electronic evidence issues. They indicate that „on 2 December 2020, the European Commission published a Communication on Digitalisation of Justice in the European Union (Communication), which outlines proposals for introducing or broadening the use of digital technology in justice systems. Fair Trials welcomes the Communication and the search for ways to make criminal justice systems more accessible. However, some of the proposed measures affect the fairness of criminal proceedings and the rights of suspects and accused persons".[65]

A long-time problem - a balance between the efficiency and guarantees of the proceedings - has been raised. Fair Trials show that „**predictive and risk-assessment AI tools target individuals and profile them as criminals before they have carried out the crime for which they are being profiled"**.[66] Such predictions can result in police surveillance, harassment and arrests, and what is more – have an impact over decisions about prosecution, bail sentencing and probation. Is should be seen as contrary to presumption of innocence rule in criminal proceedings. It is emphasised that „sufficient safeguards are needed to properly protect people's rights and freedoms against these new law enforcement and criminal justice strategies and systems, including preventing their use in certain circumstances. **AI systems must uphold the presumption of**

---

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 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".

[65] Briefing paper on the communication on digitalisation of justice in the European Union, 2021, p. 4 https://www.fairtrials.org/app/uploads/2021/11/DIGITALISATION-OF-JUSTICE-IN-THE-EUROPEAN-UNION.pdf (access: 12.10.2022).

[66] Ibidem, p. 9.

innocence. AI systems which seek to profile, predict, assess risk or otherwise pre-designate an individual as a criminal before trial must not be allowed in criminal justice".[67]

Non-content data can be divided into three groups: first - subscriber data, second - traffic data and third - location data.[68] Obtaining that kind of data is not always easy. There are more and more technological challenges such as the retention of dynamic IP addresses, 5G and Internet of Things. It shows that discussing electronic evidence issues, **we are obliged to consider not only technologies that exist right now, but also the development of technologies, their amendments and future challenges.**[69]

The „**Study on the retention of electronic communications non-content data for law enforcement**"[70] examines the national legislation and practices in respect of the following aspects, a.o.: specific retention and access needs of LEAs, in particular, which non-content data they need and for which periods of time in order to prevent, investigate and prosecute criminal offences. It is important as **the data gathered by LEAs should be limited only to these particularly relevant to the proceedings**. Practices of obtaining „as much data as possible" should be eliminated.

A „balance issue" has been also raised in the Europol and Eurojust report on encryption. Encryption helps to protect data on the Internet, but also makes it easier for criminals to communicate in secret. Obtaining encrypted data in the latter cases is important for successful fight against cybercrimes. However, the authors of the report, recognize the problem of maintaining procedural guarantees and protecting fundamental rights while obtaining such evidence in order to ensure that these data would be acceptable as evidence in judicial proceedings. Requirements of necessity and proportionality has been noticed as crucial.[71]

---

[67] Ibidem, p. 9.
[68] Study on the retention of electronic communications non-content data for law enforcement, 2020, Final report, https://www.statewatch.org/media/1453/eu-com-study-data-retention-10-20.pdf (access: 12.10.2022).
[69] Ibidem.
[70] Ibidem.
[71] Third report of the observatory function on encryption, 2021, p. 36, https://www.eurojust.europa.eu/sites/default/files/assets/joint-ep-ej-third-report-of-the-observatory-function-on-encryption-en.pdf (access: 13.10.2022).

3.2.3. Literature review

The comparison of the EIO and EPO has been presented by S. Tosza.[72] **A high need for tools to obtain cross-border electronic evidence is highlighted.**[73]

It was also stated that „inappropriate use of poorly tested technology undermines the right to a fair trial, as formulated in Art. 6 (1) ECHR and threatens the presumption of innocence at an early stage of an investigation".[74] What need to be examined is **to what extend digital evidence practices comply with fair trial principles and how technology-assisted investigations challenge criminal procedure.** R. Stoykova classifies the threats to presumption of innocence with respect to technology-assisted investigations and digital evidence in three groups:

a) inappropriate and inconsistent use of technology,
b) old procedural guarantees, which are not adapted to contemporary digital evidence processes and services,
c) the lack of reliability testing in digital forensics practices.[75]

What areas seem to be the main threat are the issues with „**reverse burden of proof, low quality data processing, reliance on untested digital expert evidence (opinion),**

[72] 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 2020, 11:2, https://journals.sagepub.com/doi/10.1177/2032284420919802 (access: 13.10.2022).

[73] 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 2020, 11:2, https://journals.sagepub.com/doi/10.1177/2032284420919802 (access: 13.10.2022); „The two instruments present significant similarities. They are two instruments with the same or similar purpose: gathering evidence using mutual recognition of orders of other member states. (...) If both instruments are available, it is difficult to imagine why authorities should not choose an EPO. Its procedure is simpler, the deadline for reaction much shorter and the pressure on execution much more significant with a set of concrete sanctions. (...) The EPOR creates a new relationship between law enforcement and private actors, that is, service providers, which, whether they like it or not, would become extended arms of law enforcement replacing their national authorities in the task of not only receiving and complying with but also assessing the orders. However, contrary to national authorities, they will do so at a threat of sanctions for non-compliance, making the service providers unreliable defenders of our fundamental rights".

[74] R. Stoykova, *Digital evidence: Unaddressed threats to fairness and the presumption of innocence*, Computer Law & Security Review 2021, 42, https://www.sciencedirect.com/science/article/pii/S0267364921000480 (access: 13.10.2022).

[75] Ibidem.

and lack of criminal procedure guarantees in data retention, crime prevention and suspicion-based procedures."[76] The example of wrongful convictions based on unreliable expert evidence are also known (Innocence Project 2020).[77] „The conclusion can be drawn that **judges have their important role in verifying the forensic evidence reliability**, but they cannot and must not perform scientific validation of digital forensic methods and tools. Their important role is to define the boundaries of permissible expert testimony in court for a particular case. (...) Therefore, there is a need for further research into the active participation of the defence during the digital forensic examination during the investigation, e.g. access to the chain of custody, the right to use the same digital forensic tools/methods to collect exculpatory evidence, the right to ask the digital forensic examiner questions, and to request scientific validation of the findings."[78] The distinction between data stored and data gathered real-time has been made what is particularly important when it comes to the tools used among EU MS to obtain these data (EIO or in the future, EPO).

The Directive's 2016/343 purpose is to enhance the right to a fair trial in criminal proceedings by prescribing common minimum rules for certain aspects of the presumption of innocence and the right to be present at trial. The scope and genesis, as well as legislative procedure of the Directive has been examined in detail in the publication „The Directive on the Presumption of Innocence and the Right to Be Present at Trial Genesis and description of the new EU-Measure."[79] Under the rule of presumption of innocence we can find several issues: **the use of compulsion, the right to remain silent, the right not to incriminate oneself, reversal of the burden of proof.** All of these aspects have been analysed and examined on the ground of the Directive in the publication indicated above. Detection of these aspects is relevant for INNOCENT, as all

[76] Ibidem.
[77] Innocence Project 2020, https://innocenceproject.org (access: 13.10.2022).
[78] R. Stoykova, *Digital evidence: Unaddressed threats to fairness and the presumption of innocence*, Computer Law & Security Review 2021, 42, https://www.sciencedirect.com/science/article/pii/S0267364921000480 (access: 13.10.2022).
[79] S. Cras, A. Erbeznik, *The Directive on the Presumption of Innocence and the Right to Be Present at Trial Genesis and description of the new EU-Measure*, EUCRIM 2016, 1, pp. 30-32

of them should be examined in the context of the kind of actions that violate these rights and standards and which ones do not.

Also, the analysis of the areas covered by digital forensic court experts has been already made.[80] It can be used worldwide to educate judges, prosecutors and lawyers that make use of the Digital Forensic (DF) experts' reports. „It illustrates what the legal community can expect from DF court experts, it provides a demarcation of the DF field based on DF literature and it presents examples of relevant questions that can or should be asked to a DF expert"[81]. The paper shows what are the DF expert areas, which experts we should use in the specific procedural situations, what questions can be asked, how to formulate these questions. The relevant questions are assigned to all of the stages of proceedings. The analysis has been made on the ground of the Dutch law system, however it can be useful in all EU MS. **Education of the judges and prosecutors, also considering ways of e-evidence verification by DF experts, is of the great value**.

The main area of research considering electronic evidence are the cross-border issues. S. Carrera and M. Stefan comparatively examined the constitutional, legal and administrative frameworks on access to and use of digital information in cross-border criminal justice cooperation in a selection of EU member states.[82] They also set out a number of policy options and practical ways forward for EU and national policy makers to promote judicial cooperation for cross-border access to and collection of electronic data in line with EU and international rule law and fundamental rights standards.

What is particularly interesting about the research paper are the examples of national judgments on the protection of fundamental rights (however, mostly right to privacy in the context of the cross-border exchange of evidence). It was - once again - stated that

[80] H. Henseler, S. van Loenhout, *Educating judges, prosecutors and lawyers in the use of digital forensic experts*, Digital Investigation 2018, 24, https://www.sciencedirect.com/science/article/pii/S1742287618300422 (access: 13.10.2022).
[81] Ibidem.
[82] S. Carrera, M. Stefan, *Access to Electronic Data for Criminal Investigations Purposes in the EU*, CEPS Papers in Liberty and Security in Europe 2020, https://www.ceps.eu/wp-content/uploads/2020/02/LSE20120-01_JUD-IT_Electronic-Data-for-Criminal-Investigations-Purposes.pdf (access: 13.10.2022).

rules on admissibility of evidence in criminal proceedings vary greatly across the Union, nor a clear EU legal framework of admissibility of evidence exists.[83]

The so-called E-evidence Legislative Package issues have been touched. It is raised in the literature that **access to effective remedies in case of fundamental rights violation** can be problematic as there are no guarantees for PSACs of the judicial control on the process of acquiring e-evidence.[84] The main concerns are caused by the lack of a duty to inform the subjects potentially affected by the proposed measure about taken actions. That seems to be contrary to existing EU privacy and data protection regulations, the principle of equality of arms and the adversarial principle in criminal proceedings.[85]

The problem of **balancing efficiency and guarantees in criminal proceedings** comes back once again, as well as the role of public authorities to protect the latter. The judicial authorities are the ones responsible for protecting and enforcing fundamental rights and freedoms. Passing the buck on the private companies might raise certain concerns. It should be agreed that mark service providers responsible for the fundamental rights protection does not seem to be a right direction.[86]

Last but not least, it has to be indicated that within the EU area, access to countries' legislation and policies exist. What can be particularly useful are these two websites:

d) https://www.coe.int/en/web/octopus/country-wiki (the wiki profiles provide an overview of a country's policy on cybercrime and electronic evidence; every fiche includes a description of cybercrime policies/strategies, the state of cybercrime legislation, the channels of cooperation, international cooperation and case law),
e) https://www.ejn-crimjust.europa.eu/ejn2021/ContentDetail/EN/6/88 (the Fiches Belges is a tool that provides practical information on specific sets of measures that are covered by judicial cooperation in criminal matters - EJN Fiches Belges on Electronic Evidence – National Legal and practical information provided by the Contact Points).

3.3. Fields to be further explored

[83] Ibidem, p. 53.
[84] Ibidem, p. 56.
[85] Ibidem, p. 56
[86] Ibidem, p. 63

3.3.1. The lack of specialised training

The in-depth analysis of electronic evidence and presumption of innocence leads to a conclusion that the topic is still under-explored and needs attention from both academics, policy makers and practitioners.

First of all, it occurred that **the lack of specialised training of judges, prosecutors, LEAs is a main threat to protection of fundamental rights** of suspects and accused, particularly when it comes to applying the presumption of innocence. This gap needs to be covered by workshops and relevant training sessions for the representatives of these professions.

What is more, **judges face difficulties when handling e-evidence in court.** It has been examined that in the past, judges seemed to be untruthful considering using electronic evidence and give a judgment basing on its content. However, the thesis of mistrust has not been validated in the later projects and surveys. To cover this knowledge gap, the relevant survey should be conducted with the right questions asked during the co-creation events in INNOCENT. It is important to know what is the judges' attitude towards electronic evidence and their impact of the final verdict. Do they perceive e-evidence in other ways than material evidence? Do they confide in them more or less than material evidence? Both extreme attitudes are dangerous - prior assumption about the credibility of the evidence causes judges' trust without any verification and prior assumption about the incredibility causes rejection of evidence without reasonable cause. Furthermore, in majority of the cases judges do not question the assessment provided by an expert witness regarding electronic evidence. The lack of scrutiny can be problematic. The attitude towards expert witness opinions should be examined here as well.

The projects mentioned in 5.1. focus mainly on the effectiveness of the proceedings, sometimes tackling the issues of the right to the privacy or the personal data protection. Rarely do they touch the opposite problem - the one of the procedural guarantees of the suspects and accused. The projects are aimed at enhancing the main actors to use the electronic evidence and not to „stay back" - rather than raising awareness of the possibilities of manipulation or need for reliability verification of the e-evidence. **Here there is a huge gap that can be covered by INNOCENT, not only during direct**

meeting but also by dissemination of the reports and recommendation paper addressed to judges, prosecutor and LEAs.

What is particularly important is to arm judges and prosecutors in the knowledge about the digital forensic court experts and how to cooperate with them, particularly: what kind of expert can be used in the specific case, and which questioned should be posed to acquire desirable knowledge. Inviting DF court experts to the workshops, webinar or co-creation meetings could be a good idea. Also, right questions should be asked during the meetings with judges and prosecutors about their experience and practices on the field of the cooperation with DF court experts. It is relevant to know in what cases judges should use such experts to verify evidence (especially credibility of non-content data) and in what cases it is inadequate and useless.

Also, the Checklist of questions (CHECKLIST GUIDANCE, FORMOBILE[87]) at the pre-acquisition stage and all of the further stages of proceedings can serve as a handbook for all the practitioners to assess the data gained from electronic devices. It can be used during workshops to raise awareness of the practitioners.

3.3.2. Preservation and verification of electronic evidence

The next field that needs to be further explored is **the way that electronic evidence are preserved and stored, in the context of presumption of innocence rule**. There are no minimum standards among EU MS as well as there are no requirements. It should be checked - during the co-creation events - if they are any common practices among LEAs from the same countries as well as among different countries. What can be seen as particularly important is to set a rule package on that to:

1. avoid files modification after possessing them and interference of the third parties,
- enable PSACs and defence lawyers to check the authenticity of the electronic evidence, the chain of custody and eventually, to challenge evidence in the court.

[87] FORMOBILE Guidance to Checklist Preparation for Legal Practitioners, https://formobile-project.eu/downloads/publications-public-deliverables/157-formobile-legal-checklist-guidance-document-final/file (access: 13.10.2022).

What seems to be equally important is **to arm judges and defence lawyers with the knowledge how electronic evidence can be verified and challenged or questioned** during judicial stage of the proceedings. Assumption of the „infallibility" of the electronic evidence violates the presumption of innocence, as their content is considered as certainty. It should be well-known information what kind of non-content data must be checked to make sure about the genesis of e-evidence. Such information should be recognised during workshops and co-creation events.

3.3.3. Presumption of innocence in the context of electronic evidence

Regarding the presumption of innocence rule on the goring of the Directive, its aspects has been detected:

1. **burden of proof,**
   - **right to remain silent,**
   - **right not to incriminate themselves.**

What should be done as a next step, is to recognise what kind of actions - during both pre-trial proceedings and judicial proceedings - violate these rights and which actions do not. Co-creation meeting seem to be a perfect space to do it by comparing practices of participating judges, prosecutors and observations made by the defence lawyers.

The **EVIDENCE** project diagnosed main obstacles regarding collecting, preserving, using, exchanging e-evidence that are mentioned above. It can be a base for INNOCENT co-creation events to ask the participants what are their ideas for overcoming that problems and obstacles and what good and bad practices they experienced. Outcome of these discussion can set a base for the recommendations addressed to law and policy makers.

Both **EVIDENCE** and **FORMOBILE** stress the need for the trainings, workshops and courses aimed at raising knowledge and awareness of the practitioners on the subject of the e-evidence and new technologies. INNOCENT will answer this need, focusing on the protection of fundamental rights the using them, not only on the technical issues of the electronic evidence.

All of the activities mentioned above should consider following distinctions of electronic evidence:

- data stored and data gathered real-time,
- content and non-content data.

It should be assumed that different rules, requirements and practices apply for evidence considering what type of electronic evidence it is.

3.3.4. New technologies

Outcomes of the EU funded projects shows that new technologies develop rapidly. Creating new solutions and policies we should taking into account not only currently existing state of play regarding new technologies, but also prefigure their development and possible interference with criminal proceedings and fundamental rights. Deliverables of ROXANNE project can be used in INNOCENT as a base for the research on **what threat when using new technologies, we should be sensitised to**. Use of dynamic Internet Protocol (IP) addresses, introduction of 5G, encryption of data, Internet of Things (IoT) and corresponding challenges should be taken into consideration during discussion and analysis within INNOCENT project.

3.4. Still unexplored

There are two areas of research that has not been covered as far:

1) effective remedies in case of violation of presumption of innocence when using electronic evidence,
2) protection of procedural rights and safeguards after EPO coming into force.

When it comes to the effective remedy issues, the question must be posed: what are the consequences of breaching the right to presumption of innocence? Most of the reports, research or publications focus on the challenge: how to avoid breaching the rights and what rules must be obeyed. Nevertheless, it has to be assumed that the rules and procedure will not always be respected, and the rights will be violated. It has to be considered, what consequences it should presuppose.

As it was stated several times, rules on admissibility of evidence in criminal proceedings vary across EU, nor a clear EU legal framework of admissibility of evidence exists. There are no rules on when electronic evidence can be used in court or not. Possible violations can have different weight and meaning. The evidence can be obtained unlawfully, they

can be directly, or indirectly illegal, fundamental rights or procedural safeguards can be breached. The **FORMOBILE** project has recognised this issue and drafted the Guidance for creation of the checklist in order to map out what is necessary to identify potential excess and non-verified use of e-evidence.[88]

It would be worth examining - after recognising what kind of behaviours and actions violate different aspects of presumption of innocence - **what are the consequences of these actions for admissibility of using e-evidence in further proceedings in different countries.** It can set a base for recognising good and bad practices and preparing recommendations for law and policy makers.

As regards to EPO, despite the fact that a lot of studies covering it exist, **there are not any analysis on the impact of the EPO on the procedural rights of PSACs**. It is particularly important as the EPOs will provide EU MS with the unknown instrument - direct contact with service providers. To some extent, this solution has been already implemented in the Protocol to the Cybercrime Convention, but the reach of it is limited to subscriber data. Acquiring data - including content data - from private actors carries a threat to fundamental rights protection. These actors are not obliged to be the guards of rights and freedoms of individuals. The impact of these new tools, ways of gathering and using electronic evidence possessed with EPO on all of the aspects of presumption of innocence, should be analysed.

4. Conclusions for the INNOCENT project

In the EU context there is a lack of publications or EU funded projects directly examining the link between electronic evidence and presumption of innocence. This gap, as anticipated, is to be covered by the INNOCENT project, using the knowledge generated upon publications and research on both electronic evidence and presumption of innocence. This will help to push forward a knowledge frontier when avoiding double-work and double-funding.

[88] FORMOBILE Guidance to Checklist Preparation for Legal Practitioners, https://formobile-project.eu/downloads/publications-public-deliverables (access: 13.10.2022).

The conclusion following from the review of the state of the art is that the most needful part of INNOCENT project are the co-creating meetings, workshops and webinars, as the lack of knowledge of the judges, prosecutors, LEAs and defense lawyers is the main obstacle when it comes to protection of presumption of innocence when using electronic evidence in criminal proceedings.

These events should be focused on:

1) technical issues concerning electronic evidence - how they should be acquired, preserved, collected, decoded, analysed stored, presented, what are the methods of interference (e.g. deleting files, recovering them, content modification) and how their authenticity can be verified,
2) cooperating with DG court experts,
3) recognising different aspects of presumption of innocence and distinguishing actions that violate them and these they do not,
4) international cooperation (both with private sector and relevant national authorities)
5) consequences of breaching the right to presumption of innocence when using electronic evidence (effective remedies).

Co-creating meetings could give a floor to the discussion, recognising above-mentioned problems, exchanging the experiences and practices among participants, when workshops and webinars could be more focused on a training session - as this is the idea behind these kinds of events.

Also, the protection of presumption of innocence aspects considering cross-border issues, future EPOs tools and development of new technologies should be detected.