Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things
Grant Agreement: 786698

D3.2 Legal analysis of the use of evidence material

Work Package 3: Legal issues: data protection and privacy

Document Dissemination Level

P	Public	☒
CO	Confidential, only for members of the Consortium (including the Commission Services)	☐

Document Due Date: 31/10/2018
Document Submission Date: 02/11/2018

Co-funded by the Horizon 2020 Framework Programme of the European Union

Document Information

Deliverable number:	**D3.2**
Deliverable title:	Legal analysis of the use of evidence material
Deliverable version:	1.2
Work Package number:	3
Work Package title:	Legal issues: data protection and privacy
Due Date of delivery:	31.10.2018
Actual date of delivery:	02.11.2018
Dissemination level:	PU
Editor(s):	Olga Gkotsopoulou (VUB) Paul Quinn (VUB)
Contributor(s):	Liza Charalambous (ADITESS) Dimitris Kavallieros (KEMEA) Xenia Pouli (MTN)
Reviewer(s):	Emanuele Bellini (MATHEMA) Clément Pavué (SCORECHAIN)
Project name:	Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things
Project Acronym	Cyber-Trust
Project starting date:	1/5/2018
Project duration:	36 months
Rights:	Cyber-Trust Consortium

Version History

Version	Date	Beneficiary	Description
0.01	20.08.2018	VUB	DDP and ToC circulated to partners
0.02	27.08.2018	VUB	Sections 1 and 2
0.021	04.09.2018	ADITESS	Contribution – clarifications integrated in Section 3
0.03	05.09.2018	VUB	Sections 3 and 6
0.04	09.09.2018	VUB	Section 5
0.05	11.09.2018	VUB	Section 4
0.06	13.09.2018	VUB	1st Internal Review
0.1	17.09.2018	VUB	Distribution of 1st draft to partners for feedback
0.2	10.10.2018	KEMEA-Hellenic Police	Input – Annex A
0.3	15.10.2018	MTN	Input – Annex B
0.4	23.10.2018	VUB	2nd Internal Review
1.0	26.10.2018	VUB	Submission for final review
1.1	01.11.2018	VUB	Final version after review by Scorechain and Mathema
1.2	14.11.2018	VUB	Updated version

Acronyms

ACRONYM	EXPLANATION
ACPO	Association of Chief Police Officers
App./appl.	Application
CERT	Computer Emergency Response Team
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CSIRT	Computer Security Incident Response Team
DLT	Distributed Ledger Technologies
DoS/DDoS	Denial of Service/ Distributed Denial of Service
DPIA	Data Protection Impact Assessment
DSP	Digital Service Provider
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ed. /eds.	Edited
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEW	European Evidence Warrant
ENISA	European Union Agency for Network and Information Security
EU	European Union
Europol	European Law Enforcement Organisation
GC	Grand Chamber
GCC	Greek Criminal Code
GDPR	General Data Protection Regulation
ICT	Information and Computer Technologies
ILOR	International Letter of Request
Interpol	International Police
IoT	Internet of Things
ISO	International Standards Organisation
ISP	Internet Service Provider
LEA	Law Enforcement Agency
MLA	Mutual Legal Assistance
MoC	Memorandum of Cooperation
NIS	Network and Information Security
No.	Number
OES	Operator of Essential Services
OJ/OJ L […]	Official Journal of the European Communities - Legislation
para.	Paragraph
pp. / p.	Pages/page
TCP/IP	Internet Protocol
T-CY	Cybercrime Convention Committee
TEU	Treaty of the European Union
TFEU	Treaty of the Functioning of the European Union

US/USA	United States of America
v	Versus
WP	Work Package

1. Introduction 10
1.1 Project Overview 10
1.2 Purpose of the Document 10
1.3 Scope and Intended Audience 10
1.4 Structure of the Document 11
2. Electronic and digital evidence as opposed to conventional evidence 12
2.1 Decipherment: electronic v digital evidence 13
2.1.1 Definition of electronic evidence 13
2.1.2 Definition of digital evidence 14
2.2 Electronic v conventional evidence: similarities and differences 15
2.3 Sources and types of electronic evidence 15
2.4 The life cycle of e-evidence and digital forensics: status quo and best practice 17
2.4.1 Definition of digital forensics 17
2.4.2 Status Quo and Best practice 17
2.4.2.1 Incident Protocols 18
2.4.2.2 Identification 18
2.4.2.3 Collection 19
2.4.2.4 Acquisition 20
2.4.2.5 Preservation 20
2.4.2.6 Examination 21
2.4.2.7 Analysis 21
2.4.2.8 Reporting 21
2.4.2.9 Expert witness testimony 22
2.4.2.10 After the criminal proceedings 22
3. Electronic evidence: the European and international framework 23
3.1 European Union 23
3.1.1 Primary law 23
3.1.2 Secondary law 24
3.1.2.1 GDPR and Directive 2016/680 24
3.1.2.2 E-privacy reform 25
3.2 Council of Europe 26
3.2.1 The European Convention on Human Rights and the case law of the Strasbourg Court 26
3.2.2 The Cybercrime Convention 29
3.2.2.1 Jurisdiction 29
3.2.2.2 Investigative powers 29
3.2.3 The CoE Recommendation 87 (15) 36
3.3 Common Principles of handling electronic evidence 37
3.3.1 The principle of data integrity 37

3.3.2 The principle of audit trail 38
3.3.3 The principle of specialist support 38
3.3.4 The principle of appropriate training 38
3.3.5 The principle of legality 38
4. Electronic evidence: national frameworks 39
4.1 National frameworks of relevance for CYBER-TRUST 39
4.1.1 Cyprus 39
4.1.2 Greece 40
4.1.3 Italy 41
4.1.4 Luxembourg 42
4.1.5 The Netherlands 42
4.1.6 United Kingdom 43
4.1.7 USA 44
4.2 Relevance to CYBER-TRUST 44
5. Cross-border access to electronic evidence 49
5.1 Exchange of electronic evidence across Europe 49
5.1.1 European Union 49
5.1.1.1 Primary law 49
5.1.1.2 Secondary law 49
5.1.1.2.1 The Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 2000 51
5.1.1.2.2 The Directive on the European Investigation Order (EIO) 52
5.1.1.2.2.1 Cyprus 54
5.1.1.2.2.2 Greece 54
5.1.1.2.2.3 Italy 54
5.1.1.2.2.4 Luxembourg 55
5.1.1.2.2.5 The Netherlands 55
5.1.1.2.2.6 United Kingdom 55
5.1.1.2.3 Europol and Eurojust 55
5.1.2 Why is the regulatory framework so complex and why is new legislation in EU needed? 56
5.1.3 New proposed electronic evidence framework 58
5.2 Transfer of electronic evidence to/from third countries 59
5.2.1 The CoE Cybercrime Convention 59
5.2.1.1 Mutual Assistance 60
5.2.2 New proposed framework 60
5.3 At the national level 61
5.4 Relevance to CYBER-TRUST 61
6. The legal dimensions of the use of DLT systems for the storage of evidentiary material 63

6.1 Definitions 63
6.2 Features of the DLT system 64
6.2.1 Actors 64
6.2.2 Layers 64
6.2.3 Consensus algorithms 65
6.2.4 Understanding centralisation v decentralisation 66
6.2.5 Design choices 66
6.3 Implications with the European legal framework 67
6.3.1 Lack of *ad hoc* regulation 67
6.3.2 GDPR considerations 68
6.3.2.1 Personal data 68
6.3.2.2 Data controllers and processors 70
6.3.2.3 Jurisdiction and territoriality 71
6.3.2.4 Enforcement of data subject´s rights 71
6.3.2.5 Data protection by Design and by Default 72
6.3.2.6 Smart contracts 73
6.3.2.7 Off-chain v On-chain considerations 74
6.3.2.8 Data security 75
6.3.2.8.1 Private keys 75
6.3.2.8.2 Censorship resistance and 51% attacks 75
6.3.3 Chain of custody 75
6.4 Relevance to CYBER-TRUST 76
7. Conclusions 79
7.1 Overview of the implications for CYBER-TRUST 79
7.1.1 Admissibility of evidentiary material 79
7.1.2 Cross-border access to electronic evidence 80
7.1.3 Use of DLT systems for the storage of evidentiary material 80
7.2 Final remarks 81
Annex A – Case study: investigation of a DDoS attack in Greece 82
Annex B - Case study: Telecommunications service provider incident management procedure 84
8. References 85
8.1 Literature 85
8.2 Case law 86
8.3 Documents of European Organisations 86
8.4 Documents of International Organisations 88
8.5 European Legislation 89
8.6 Other sources 90

Executive Summary

A definition of **electronic evidence** which is broad enough to include all kinds of evidence regardless of their origin reads as follows: "Electronic evidence is any data resulting from the output of an analogue device and/or a digital device of potential probative value that is generated by, processed by, stored on or transmitted by any electronic device." **Digital evidence** is a subset of electronic evidence. The latter can take several forms and comes from various sources. Despite having some similarities with the conventional types of evidence, electronic evidence is higly volatile, can be manipulated easily, requires the use of special tools and a higher degree of technical and legal expertise. Its life cycle starts with its identification and finishes with its documentation and reporting. **Digital forensics** is defined as the "process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e., a court of law)." Different branches have been developed over the years, including computer, network and mobile forensics. Digital forensics, based on legislation, standardised procedures and protocols, attempt to guarantee the proper handling of electronic evidence throughout its life-cycle.

For there exists **no comprehensive international or European legal framework** in relation neither to evidence nor electronic evidence, the collection, preservation, use and exchange of **electronic evidence relies on the national law**. For criminal matters, those provisions are usually found in the criminal law and the criminal procedural law. Few countries have adapted their legislation to accommodate electronic evidence. However, the majority relies on old laws which apply to electronic evidence by analogy. There are thus **significant differences in national legislations and approaches**, which makes the handling of electronic evidence complicated across jurisdictions. All in all, legislation requires a clear scope of application of powers and sufficient legal authority for actions, but the conditions may vary considerably even in countries with the same legal tradition. Albeit, **a number of international and European legal instruments and policy documents are relevant to electronic evidence**, including EU legal initiatives and guidelines, and the legal instruments and documents by the Council of Europe.

It is highly recommended to follow the principles introduced in the CoE Electronic Evidence Guide and the ENISA´s Handbook on Digital Forensics concerning the proper handling of electronic evidence, which comprise the fundamental common principles found in the vast majority of national legislations: **a. data integrity**, ensuring no alterations either to software or hardware; **b. audit trail**: documenting all actions; **c. specialist support**: consultancy with external experts; **d. appropriate training**: first responders must be appropriately trained; **e. legality:** ensuring that the law and the general procedural principles are taken into consideration. The material must be treated in such a manner that will give the best opportunity for any recovered data to be admissible as evidence in later proceedings **in accordance with the domestic law requirements**, both of the state where the proceedings take place and the state where the information was collected from.

Since cybercrime knows no borders, the main instruments shaping the current **legal framework for cross-border access to evidence** consists of bilateral and multi-lateral mutual legal assistance (MLA) instruments, the European Investigation Order (EIO), the Budapest Convention, and national laws and procedures of Member States and third countries. Cross-border access to electronic evidence may be achieved through formal cooperation between the relevant authorities

of two countries, usually via an MLA or an EIO (between the EU Member States), or police-to-police cooperation; through direct cooperation between law enforcement authorities of one country and service providers whose main establishment is in another country, either on a voluntary or mandatory basis; through direct access, if provided for by the national law. Nevertheless, the regulatory framework at EU and at Council of Europe level is under **intense reform**, since the current framework was proved to be too slow, complex and inefficient for today´s law enforcement needs. The CYBER-TRUST consortium has to take into consideration the international, European and national framework, as well as the guiding principles and best practices throughout the gathering and handling of material that may contain electronic evidence, in order for it to have a greater chance to be admitted in the different jurisdictions.

The terms "**Distributed Ledger Technology**" and "**Blockchain**" are often used interchangeably. Distributed Ledger Technology is an umbrella term for the underlying technology, whereas Blockchain was the first fully functional system, hence, simply a DLT subcategory. A DLT system is defined as "a system of electronic records that enables a network of independent participants to establish a consensus around the authoritative ordering of cryptographically-validated ('signed') transactions. These records are made persistent by replicating the data across multiple nodes, and tamper-evident by linking them by cryptographic hashes. The shared result of the reconciliation/consensus process - the 'ledger' - serves as the authoritative version for these records." The system consists of a protocol layer, a network layer and a data layer and this ordering reflects conceptual and functional dependencies. **In criminal proceedings, DLTs could be used to track the chain of custody when evidence is captured, gathered and taken for analysis.** Design choices, for instance, giving preference to centralised or decentralised solutions, choosing a permissioned or permissionless type of DLT, or keeping an off-chain record would lead to different legal considerations, given the different characteristics of each system and could make compliance with GDPR and privacy frameworks easier or impossible. Prior to any implementation, detailed threat models and specific security requirements need to be identified, in order to determine what design fits better the needs of CYBER-TRUST, in accordance with the existing regulatory framework and the principles of data minimisation and data protection by design and by default.

The biggest challenges concerning the use of DLT for the storage of electronic evidence are a. the lack of ad hoc regulation, since the technology is still in its infancy, b. the compliance with the GDPR in relation to personal data stored on- or off-chain, c. the identification of data controllers and processors, d. the determination of jurisdiction, e. the enforcement of data subjects´ rights, f. the implementation of appropriate organisational and technological measures, g. the use of smart contracts, h. the data security, and i. the admissibility of evidentiary material grounded on a DLT-based chain of custody. These hurdles may be eliminated in the near future, with the evolvement of relevant case law and the issuance of specific guidelines resulting in more legal certainty, as well as the creation of novel GDPR-compliant technical solutions.

1. Introduction

1.1 Project Overview

CYBER-TRUST | Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things is a 36-month long research project in the Digital Security Focus Area, co-funded by the Horizon 2020 Framework Programme of the European Union, under the Grant Agreement no. 786698. Its principal goal is to revolutionise the way cyber-security systems are built and operate.

By establishing an innovative cyber-threat intelligence gathering, detection, and mitigation platform, as well as, by performing high quality interdisciplinary research in key areas, the CYBER-TRUST project aims to develop novel technologies and concepts to tackle the grand challenges towards securing the ecosystem of IoT devices. It is structured around three pillars: a. key proactive technologies, b. cyber-attack detection and mitigation, and c. distributed ledger technologies.

1.2 Purpose of the Document

The present deliverable (D3.2), the second of five, is part of the Work Package 3 (WP3). The latter aims to navigate the legislative requirements that are applicable to the project, provide recommendations during the platform design, and conduct a Data Protection Impact Assessment (DPIA), in accordance with Article 35 of the EU General Data Protection Regulation (GDPR).

The D3.2 is also, specifically, the outcome of task T3.2, which focuses on the legal requirements relating to the collection, processing and use of evidence for criminal proceedings and judicial matters. Rules pertaining to evidence collection, admissibility and processing are in general governed by national law, whilst the relevant European and international legislation are at the moment under intense reform.

This task will conduct an analysis of the main applicable principles in terms of relevance to the CYBER-TRUST project and will focus on the concrete legal requirements of EU Member States, with direct relevance to the project, as well as some other key EU players in the area of cybersecurity. After D3.2, the next deliverable D3.3 will attempt to determine the requirements that are likely to be applicable to the type of services envisaged by the CYBER-TRUST project, based on the framework established by the two previous deliverables.

The material produced from this task will feed into tasks T6.2 (and the respective deliverables D6.2; D6.6) and T6.3 (and the respective deliverables D6.3; D6.7) that deal with the detection and mitigation of device and network attacks respectively, as well as tasks T7.2 (and the respective deliverables D7.2; D7.3) and T7.4 (and the respective deliverable D7.5) that will define the use of the DLT system with forensic evidence.

1.3 Scope and Intended Audience

The intended audience of the document are the project stakeholders and the project team (Consortium staff). According to the preliminary security scrutiny, this deliverable is classified as PU = Public.

1.4 Structure of the Document

Section 2 presents the definition of electronic evidence, as opposed to conventional evidence. In this part, we decipher the particularities of electronic evidence and digital evidence, understand the sources and types of electronic evidence. Sections 3 outlines the international and European framework concerning electronic evidence, while Section 4 focuses on the national framework in selected Member States of relevance for CYBER-TRUST, with emphasis to the admissibility of electronic evidence and national investigative powers in criminal proceedings. Section 5 gives insight into the complex legal system of exchange and transfer of electronic evidence. Section 6 introduces the discussion around the use of DLT systems for the storage of electronic evidence. Section 7 concludes with an overview of the implications for CYBER-TRUST, based on the relevant Sub-sections, and provides the final remarks.

2. Electronic and digital evidence as opposed to conventional evidence

The world becomes constantly more and more digitized. At the same time, thousands of security incidents on networks and attacks against computer systems and data infrastructures are recorded worldwide. Cybercrime, however, is not merely a matter of attacks against machines.[1] It entails a serious threat to the fundamental rights of individuals, to the rule of law and to democratic societies. Cybercrime is, however, still underreported, whilst from the reported cases, only a small part is investigated and prosecuted.[2] A detailed analysis of the different categories of cyberthreats can be found in D2.1. What becomes apparent is that no area stays intact from cyber attacks, be it healthcare, smart homes, industry or even physical security.

With such a big spectrum of action, the activities of cybercriminals both in the offline and online sphere can generate an incredible number of digital trails, which can be valued as electronic evidence, proving innocence or guilt, sometimes with greater accuracy and sometimes with lesser. Electronic evidence is relevant not only to cybercrime but to almost any type of crime in one way or another. 85% of criminal proceedings in Europe seem to rely on electronic evidence stored in servers locally or abroad, while evidence coming from traditional sources is also most of the times stored in digital form.[3]

The growing significance of electronic evidence becomes even more apparent in view of the increasingly international dimension of crime. Law Enforcement Agencies (LEAs) must, therefore, adapt to the rapid development of technology and implement effective ways to handle electronic evidence. The CYBER-TRUST, grasping the need for such solutions, in particular with regards to the widespread use of Internet of Things (IoT) applications, aims to provide a tool, which not only enhances cyber-threat intelligence gathering and sharing for the prevention and mitigation of cybercrime but also supplies a DLT-based platform enabling the storage and documentation of material that contains potential evidence.

Given the particular circumstances under which cybercrime occurs and is mitigated, as well as the distinctive features of electronic evidence, which still does not have a unified commonly accepted definition, prominent legal debates arise. Questions of admissibility with regards to the obtained evidence are quite often since there is no clear legal principle to which the judge can refer to, in order to determine the admissibility of specific evidence. This uncertainty can result in the inconsistent or unbalanced application of the existing law. Moreover, the rapid evolution of forensic technologies and the manipulability of electronic records hinders the efforts for achieving a standardisation model,[4] while the globalisation of crime requires close, constant and efficient cooperation among police forces and judicial authorities of different countries with different legal systems, administrative processes and technological standards.

[1] Council of Europe, Enhanced international cooperation on cybercrime and electronic evidence: Towards a Protocol to the Budapest Convention, 2 November 2017, p.151.
[2] Brown CSD (2015) Investigating and Prosecuting Cyber Crime: Forensics Dependencies and Barriers to Justice, International Journal of Cyber Criminology 9, pp. 55–119.
[3] Ibid.
[4] Sethia, A. (2016), Rethinking admissibility of electronic evidence. International Journal of Law and Information Technology, 24(3), pp. 229–250.

The following sub-sections will attempt to answer some of the questions around electronic evidence pertaining to the development of the CYBER-TRUST prototype. First, provided the international character of the topic, the document will attempt to provide a definition of electronic evidence as opposed to conventional evidence coming from traditional sources and clarify upon the term digital evidence. Further, the discussion will focus on the various stages in the "life cycle" of evidence, from its collection and preservation until its admissibility before a court. This part will be concluded with a discussion around the impact of electronic evidence on police matters and judicial proceedings.

2.1 Decipherment: electronic v digital evidence

Comparative studies of the legal systems of European countries showed that there is no comprehensive international or European legal framework with regards to electronic evidence and although some states were found to contain references to such a concept, they did not have a specific definition of the electronic and/or digital evidence.[5] It is also highlighted that quite often under the legal systems in question, the evidentiary material in electronic form, such as electronic documents, electronic signatures and electronic communications are treated by analogy as their more conventional counterparts.[6] However, worldwide there have been many interdisciplinary attempts to define electronic and digital evidence.

2.1.1 Definition of electronic evidence

The International Organization on Computer Evidence (IOCE) views the electronic evidence as "information generated, stored or transmitted using electronic devices that may be relied upon in court",[7] whereas Mason defines electronic evidence as "data (comprising the output of analogue evidence devices or data in digital format) that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system, that is relevant to the process of adjudication".[8] Electronic evidence may include evidence in the form of analogue data, for example, video and audio tape recordings. Albeit, this data did not originate in digital form. The EVIDENCE Project,[9] adopted a definition of electronic evidence which is broad enough to include all kinds of evidence regardless of their origin: "Electronic evidence is any data resulting from the output of an analogue device and/or a digital device of potential probative value that is generated by, processed by, stored on or transmitted by any electronic device."[10] The term data includes any analogical or digital item, as the output of analogue devices or other data in digital form.[11]

[5] Insa, F., The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime-Results of a European Study, in Journal of Digital Forensic Practice, 2006, p. 285.
[6] Ibid.
[7] Chapter I, Introduction to Digital Forensics, available at: https://docplayer.net/51833294-Introduction-to-digital-forensics.html (accessed September 09, 2018).
[8] Mason, S. (2008), International Electronic Evidence, British Institute of International and Comparative Law, p.xxxv.
[9] EVIDENCE Project, Horizon 2020-funded initiative from the European Commission to collect information concerning the handling of electronic evidence in European Union.
[10] EVIDENCE project, Final Report Summary (European Informatics Data Exchange Framework for Courts and Evidence), *cordis.europa.eu*
[11] COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal

2.1.2 Definition of digital evidence

According to Mason who has conducted an extensive study concerning the law of evidence in Europe and other continents,[12] even though the terms "electronic evidence" and "digital evidence" are usually used interchangeably, the latter is a subset of the first.[13] Digital evidence is defined by the EVIDENCE project as "that electronic evidence which is generated or converted to a numerical format."[14] The Scientific Working Group on Digital Evidence (SWGDE) defines digital evidence as "information of probative value stored or transmitted in digital form".[15]

Casey defined digital evidence as "any data stored or transmitted using a computer that supports or refutes a theory of how an offence occurred or that addresses critical elements of the offence such as intent or alibi".[16] Mason classified digital evidence into three distinct categories:[17]

a. User-generated digital evidence: all digital data resulting from human action or intervention. This category of evidence may be further divided into two subsets: human-to-human, as in the case of e-mail correspondence which implies an interaction between at least two human beings; and human-to-machine, as in the case of the document when using a document editing processor.
b. Computer-generated digital evidence: all output of software programs, generated in accordance with specific algorithms and without human intervention, for instance, data recorded through electronic intercepts.
c. Digital evidence generated by both computers and users: all data resulting from human input and electronic processing, subsequently stored in an electronic memory system, for instance, a spreadsheet with results on calculations carried out by the user.[18]

Although the CYBER-TRUST prototype, will most likely be concerned with the gathering and handling of what could be defined as "digital evidence" originating from the analysis of cyberthreats and the mitigation of cyberattacks, we choose to use the term "electronic evidence" for reasons of consistency with the existing and proposed legal frameworks of the European Union, where the term electronic evidence seems to be preferred. Furthermore, the term "electronic evidence" is broader and provides a better ground for the development of a research project, without limiting its scope.

proceedings, SWD/2018/118 final - 2018/0108 (COD), p. 3. Definition of electronic evidence in the Glossary: electronically stored data such as subscriber information, metadata or content data, generated by any activity related to digital service.

[12] Mason, S. (2007), Electronic Evidence - Discovery & Admissibility, LexisNexis Butterworths, London, paragraph 2.03.

[13] Chapter I, Introduction to Digital Forensics, available at: https://docplayer.net/51833294-Introduction-to-digital-forensics.html (accessed September 09, 2018).

[14] EVIDENCE project, Final Report Summary (European Informatics Data Exchange Framework for Courts and Evidence), *cordis.europa.eu*

[15] Ibid.

[16] Chapter I, Introduction to Digital Forensics, available at: https://docplayer.net/51833294-Introduction-to-digital-forensics.html (accessed September 09, 2018).

[17] Ibid.

[18] Ibid.

2.2 Electronic v conventional evidence: similarities and differences

Criminal proceedings depend on evidence and traditionally, evidence has been in physical form, or it consisted of the oral testimony of witnesses. Electronic evidence is derived from electronic devices such as computers, networks, mobile devices, digital cameras and other digital equipment, as well as from the Internet. In many ways, electronic evidence shows some similarities with traditional evidence in that the party bringing it into the legal proceedings carries the burden to demonstrate that it is valid and authentic. To that end, documentation of each and every step, like in the case of conventional evidence, is crucial.

Comparing traditional evidence with electronic evidence,[19] the conclusions are that a number of differences can be identified. [20] First, the extraction of electronic evidence often requires the intervention of experts and the use of special tools, since electronic evidence can be invisible to non-experts. Second, it is highly volatile, meaning that in some devices, computer memory might be overwritten or changed, just by casually using the device or may be corrupted by the loss of power. Moreover, the state of the computer memory can be changed at the user's request even remotely or automatically by the operating system. High volatile also entails that some types of evidence might exist only for some seconds. Third, digital information can be copied indefinitely or can be copied at another means, meaning that experts can examine the copy instead of the original one ensuring that the original one remains unaffected. Another characteristic of electronic evidence may also be its transnationality since the data or device in question may be found in one or many different jurisdictions or even in the hands of third private entities.

As explained above the extraction of electronic evidence may require the intervention of experts. Proper handling of electronic evidence implies a higher degree of know-how concerning very complex technical and legal frameworks, compared to conventional evidence: the electronic evidence must at all stages be processed by specialists, since every piece of information or device has its own special features that call for specific attention and skills, as well as the application of appropriate and approved procedures, techniques and tools ensuring the integrity of the information and the avoidance of any unintentional alterations. Moreover, with the continuous evolution of new technologies, electronic evidence can be extracted from more divergent sources, demanding for procedures, tools and techniques to also keep up with the technological development at a very quick pace. The tools and procedures used to safeguard the potential evidentiary value of the collected material must be traceable, auditable and repeatable by other forensics specialists with the same final result.

2.3 Sources and types of electronic evidence

Investigators should always treat the electronic devices and other electronic equipment or systems as if they possibly include evidentiary material. The variation in devices and systems containing electronic evidence increases steadily every day especially with the development of IoT ecosystems. Therefore a list of sources and types can never be exhaustive but only indicative. Computer systems have different components, both hardware and software and they have different forms, such as

[19] Biasiotti, et al. (2018), Handling and Exchanging Electronic Evidence Across Europe, Springer International Publishing, pp. 4-5.
[20] Council of Europe, Electronic Evidence Guide, A basic guide for police officers, prosecutors and judges, Strasbourg, 15 December 2014, p.12.

laptops, tablets or supercomputers, while a plethora of devices will be connected to them, such as routers, printers or even coffee machines and power grids.

The Budapest Convention on Cybercrime of the Council of Europe provides the definition of "computer system" and "computer data" in Article 1, covering a big range of computer systems, such as tablets, smartphones and other devices:

a. 'computer system' means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b. 'computer data' means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function[.]

At the EU level, the Directive 2013/40 on attacks against information systems,[21] even though it repeats the definition of computer data as read in the Cybercrime Convention, introduces the definition of "information system" in Article 2, using as a basis the Convention definition of "computer system":

(a) 'information system' means a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance[.]

Electronic evidence as a generative term can come in many forms.[22] The first type is physical or traditional (not electronic) evidence such as a murder weapon, which is digitised, for example, by taking a digital photograph. The second type is analogical evidence, that is evidence in an analogue form which is digitized, acquiring a digital status, for instance the photograph of a bloodstain. The third type of evidence is digital evidence, that is, evidence originally in digital form as created by any digital device or a network.[23] Digital evidence, in turn, can also take physical or logical form: the physical form refers to the construction and resultant appearance, in the form of a physical component or digital device that contains potential digital evidence, whereas the logical form refers to the format of the data and its storage location within the digital device or a network.

[21] 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, p. 8–14.

[22] The distinction was provided by the EVIDENCE project.

[23] The EVIDENCE Project considers all these forms of evidence as 'electronic evidence', taking into account that at the end of the process they can be labelled as electronic regardless of their origin.

2.4 The life cycle of e-evidence and digital forensics: status quo and best practice

2.4.1 Definition of digital forensics

One definition of digital forensics reads as follows: "the process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e., a court of law)."[24] Another definition reads: "The application of digital investigation and analysis techniques to perform a structured examination of a digital storage medium, while maintaining a documented chain of evidence, for the purpose of gathering information admissible in evidence in a court of law or in a disciplinary procedure."[25]

Nowadays, different branches of digital forensics have been developed.[26] The oldest discipline of digital forensics is computer forensics which focuses on gathering evidence from a computer or associated digital storage device, by preserving, developing, recovering, analysing or merely presenting facts. The original device may or may not be removed; a disk image of the device may be created; erased files may be recovered.[27] A relatively new field is the network forensics, which focuses on monitoring and analysing computer network traffic. Digital forensics analysts can review network communications from various sources such as content downloading platforms and game consoles. The aim is to collect evidence of exceeding authorisation or detect intrusion in a specific system or network.[28] Due to the volatile and dynamic nature of the network traffic, two approaches to gathering information are currently applied: a. a more traditional approach which catches and stores indiscriminately all data for analysis at a later stage; and b. a less traditional approach which scans the data that passes through the network and is selective about which data is captured and therefore, the possibility to collect personal data or confidential information is minimised.[29]

Another branch of the digital forensics is the mobile device forensics. This field of forensics poses big challenges, due to memory volatility and includes an examination of cell phones, Universal Serial Bus (USB) drives, personal digital assistants, global positioning systems (GPSs), and other devices of daily use. Data that can be collected during such processes include, but are not limited to, contacts, email and social media communications, web browsing information, photos, and geolocation.[30] [31] To those branches can also be added the memory forensics and the malware forensics.[32]

2.4.2 Status Quo and Best practice

Digital forensics include a number of steps, which reflect the life-cycle of electronic evidence, as seen in Section 2.4 and must be taken with the necessary caution, so as not to reduce or eliminate

[24] Mohay, G. M. et al. (2003), *Computer and Intrusion Forensics,* Artech House, USA.
[25] European Anti-Fraud Office (OLAF), Guidelines On Digital Forensic Procedures For OLAF Staff, 15 February 2016, p.1
[26] Cybersecurity Nexus, Overview of Digital Forensics, *infosecurityeurope.com*, p.10-11.
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Ibid.
[31] Ibid. "Call records and mobile backups can also be obtained through carriers, which provide other information that is useful in developing evidence, especially in cases of encryption. Encryption can be defeated, but modifying the user's data in order to obtain the encryption keys can cause trouble from a technical and legal point of view."
[32] Biasiotti, M. et al., p.7.

the probative value of the allegedly evidentiary material.[33] Different approaches use different names or different numbering, but the core procedure remains the same. There are different ways that improve the chances for admissibility of evidence regardless of the requirements of each specific jurisdiction, such as implementing ISO (International Standards Organisation) protocols, obtaining professional training and certifications, developing an *ad-hoc* code of conduct and following approved guidelines, for instance, the ACPO Good practice guide (further discussed in Section 4.1.6) or the ENISA digital forensics handbook. Even though a need for standardisation for this rather young field of forensics concerning the handling of electronic evidence seems to be prominent, the following description constitutes a compilation of common and best practices per step in a forensic analysis process in Europe and at a global level. The following distinction is based on the overview proposed by Hamidovic (2016), which is in line with the life-cycle of electronic evidence as introduced by the EVIDENCE project.[34]

2.4.2.1 Incident Protocols

Once a cyber-attack has been mitigated, or a cyber-threat has been identified, the crime scene must be secured, non-contamination precautions must be taken and the proper authorisations must be acquired for the full investigation to start. The first challenge is to retain and document the state and integrity of the critical items (digital or not) that may carry or be evidentiary material. Protocols will be activated, best practices must be followed, and valid procedures must be carried out in order to minimise the chance of errors or mishandling of evidentiary material. Whoever is responsible for securing a crime scene, whether first responders or electronic evidence examiners, should be trained to follow accepted protocols, ensuring that the scene is secure, all contents are mapped and documented, and the followed process was fully reported.[35] Unauthorised persons should be prevented from having access to devices which may contain evidentiary material. In the case of a network which is a potential use case in CYBER-TRUST, a crime scene may include evidence in a network stored in various locations, making it difficult or impossible to reach.[36] In that case, the network forensics examiners may model sessions of traffic flows and detect anomalous patterns, which will lead them to the final decision whether the traffic is anomalous or not. The examination has to be in accordance with privacy and data protection rules, in a case-by-case assessment always with respect to the requirements of necessity and proportionality and upon the right authorisation.

2.4.2.2 Identification

As discussed in Section 2, electronic evidence may be found in various forms, physical and logical. "The identification process involves the search for, recognition and documentation of potential electronic evidence at an incident scene".[37] This stage also includes a triage process to assess

[33] Casey, E. (2011), Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press, Inc., Orlando, FL, USA.
[34] Hamidovic, H. et al. (2016), The basic steps of digital evidence handling process, International Journal of information and communication technologies, Vol. 2.
[35] Ibid.
[36] Divakaran, D.M., et al. (2017), Evidence gathering for network security and forensics, Digital Investigation Vol.20, Supplement (March 2017), pp. S56-S65.
[37] Hamidovic, H. et al. (2016).

volatility and prioritise collection, so as for potential damage to be minimised.[38] Hidden material which may contain potential electronic evidence must also be detected, including information which might not be easily located, for example, cloud computing evidence or anomalous patterns in a network.

2.4.2.3 Collection

When the critical devices or virtual spaces have been identified, cleared and framed, first responders or electronic evidence examiners should decide whether to collect the potential evidentiary material and if yes, whether they should do that physically or virtually.[39] Depending on the decision, different safeguards will have to be implemented. For instance, sometimes removing a device could sometimes cause unnecessary hassle.[40] In that case, a different approach should be followed. Except for the critical device or any other piece of electronic evidence, it might be as well necessary to collect any other material that might assist with the analysis and examination of the main material.[41] Given the big importance of this stage, because depending on the methods and tools used, alleged electronic evidence may be easily tampered or spoofed, first responders or electronic evidence examiners should always consider the following circumstances.[42] [43]

First, they should make sure that they have the legal entitlement to collect the evidentiary material in the first place and that they use the least intrusive or disruptive method to do so. In addition to that, the first responders or electronic evidence examiners should reflect on whether the implemented measures are considered legal by the specific jurisdiction where the evidentiary material is located as well as where the evidentiary material is going to be used.[44] The responders must also consider whether the removal of a digital device could create a life-threatening situation, could disrupt the regular business of an enterprise or constitutes part of critical infrastructure.[45] Moreover, the responders have to take into account whether the collection must happen as fast as possible or can be postponed for later and if volatile data or encrypted data is contained.[46] It is also important to clarify the ultimate aims of such a collection. For instance, different techniques will be used if the responders or the examiners wish to follow and trace the operational methods of a suspect during the alleged attack or the operation happens after the alleged attack.[47]

In practice, investigative measures which are most often legally permitted and used by Law Enfrocement Agencies for the identification and collection of electronic evidence in Europe are the search and seizure of digital data, including real-time interception of content or traffic data wherever this is permitted by national law, and/or hardware as well as the order to supply stored content data, stored traffic data and/or identity or subscriber information.[48] The least used or

[38] Ibid.
[39] Ibid.
[40] Casey, E. (2011).
[41] Hamidovic, H. et al. (2016).
[42] Ibid.
[43] Ibid.
[44] Ibid.
[45] Ibid.
[46] Ibid.
[47] Ibid.
[48] Biasiotti, M. et al. (2018), p.82.

prohibited investigative measures include remote access to data, covert online investigations and geolocation tracking.[49]

2.4.2.4 Acquisition

"The acquisition process involves producing an image of potential electronic evidence or of a digital device that may contain potential electronic evidence and documenting the methods used and steps taken".[50] From a wide range of methods and tools, the first responders or electronic evidence examiners should use the most appropriate one and be able to justify this choice.[51] The original piece and the image copy should be tested with a commonly accepted verification process, that is also acceptable by the jurisdiction where the evidence will be used.[52] If the verification process is difficult, for example due to errors in the original piece, first responders or electronic evidence examiners should use the best possible alternative available. If verification is truly impossible, then the reasons and the circumstances have to be fully documented and justified.[53] Data minimisation techniques in the acquisition phase should always be preferred and particular considerations for the right authorisation should be made when it is likely that the material contain personal data.[54]

In practice, the acquisition of electronic evidence in Europe is carried out by the LEAs´ in-house digital forensics specialists or labs. In some cases, external private forensics experts or labs may also contribute, in particular when there is a lack of in-house experts or tools.[55]

2.4.2.5 Preservation

Potential electronic evidence should be preserved for the protection of the integrity of the evidence. This step is particularly crucial before a lengthy Mutual Legal Assistance (MLA) process starts, for instance, in cases with a cross-border element.[56] The preservation process involves the safeguarding of potential electronic evidence and of digital devices that may contain potential electronic evidence from tampering or spoliation. The preservation process should be initiated and maintained throughout the electronic evidence handling, starting from the identification phase. In the best-case scenario, there should be no spoliation to the data itself or any metadata associated with it (e.g. time-stamps). First responders or electronic evidence examiners should be able to demonstrate that the evidence has not been modified since it was identified.

In most cases in Europe, the confidentiality of electronic evidence is a requirement, either a business requirement (e.g. the service provide which has the evidentiary material in its possession must keep the process confidential) or a legal requirement (e.g. privacy or data protection regulation). Concerning the storage of the evidentiary material, it appears uncommon practice to

[49] Ibid.
[50] Hamidovic, H. et al. (2016), The basic steps of digital evidence handling process, International Journal of information and communication technologies, Vol. 2.
[51] Ibid.
[52] Ibid.
[53] Ibid.
[54] Ibid.
[55] Biasiotti, M. et al. (2018), p.88.
[56] Ibid.

subcontract the storage of electronic evidence to third parties. Instead the responsibility of storing it, most often, lies with the Law Enforcement Agency.

2.4.2.6 Examination

Examination and analysis can sometimes be regarding as two overlapping processes. Nevertheless, an in-depth systematic examination of evidence relating to the suspected crime needs to be conducted prior to performing the full analysis.[57] This step includes identifying the smallest set of digital information that has the highest potential for containing data of probative value and documenting in detail this process for the next step of the scrutinised analysis.[58]

2.4.2.7 Analysis

In this phase, the detailed study of the data identified in the examination step is carried out.[59] After several rounds of examination and analysis, the examiners should be able to determine the significance of this piece of information or device for the overall case and draw conclusions, which may not always be straightforward, in order to reach a well-supported crime theory.[60]

In Europe, the two forms of examination and analysis most often used are computer forensics and mobile device forensics.[61] Live, network and malware forensics are also carried out by most LEAs, whereas cloud forensics and remote forensics are the least performed, not regulated or even prohibited. The relevant examination and analysis activities seem to be carried out in their vast majority by the LEAs a*d hoc* trained and experienced staff and less by external private partners.[62]

2.4.2.8 Reporting

Final reports guarantee the transparency of the investigation process. The reports may contain documentation from each phase of the process, including mentions of the protocols followed and the methods used to perform all the aforementioned steps, as well as all the necessary legal authorisation acquired and the organisational and technical safeguards put in place.[63] Reporting is not always a separate step, as it usually takes place in parallel with all the investigative activities.[64] Also, a good report would describe alternative methods that were eliminated, theories that were rejected, and in general, information that could support the examiner's objectivity towards the case to the greatest extent possible.[65] The necessity and proportionality of the collection method should be assessed as well, and it has to be proven that only information which was entirely relevant to the investigations in question was captured and collected, whereas any other data collaterally captured and not used for the investigations was erased immediately.

[57] Hamidovic, H. et al. (2016).
[58] Ibid.
[59] Casey, E. (2011).
[60] Reith, M. et al. (2002), An Examination of Digital Forensic Models, International Journal of Digital Evidence Volume 1, Issue 3.
[61] Biasiotti, M. et al. (2018), p.86.
[62] Ibid.
[63] Hamidovic, H. et al. (2016).
[64] Ibid.
[65] Casey, E. (2011).

2.4.2.9 Expert witness testimony

In some jurisdictions, the investigator as an expert witness may have to present the findings outlined in the report and address related questions, before the court can reach a conclusion. In that case, technical issues have to be explained in a clear and understandable manner.[66]

In Europe, the LEAs may be invited to provide expertise before a Court. Findings are usually presented in a very simple way, due to the low level of technical knowledge of the judges, the prosecutors and the jury.[67]

2.4.2.10 After the criminal proceedings

Last but not least, there should always be a consideration as to what will happen to the evidence after its use for the criminal proceedings.[68] If the material is no longer definitively needed, then it can be erased. If the material may be needed for further proceedings, then it should be stored securely, under the same conditions of its first storage, in line with the internal regulations of each agency.

[66] Casey, E. (2011).
[67] Biasiotti, M. et al. (2018), p. 86.
[68] Reith, M. et al. (2002).

3. Electronic evidence: the European and international framework

There exists no comprehensive international or European legal framework in relation neither to evidence nor electronic evidence.[69] The collection, preservation, use and exchange of electronic evidence, in principle, relies on the national law. For criminal matters, those provisions are usually found in the criminal law and the criminal procedural law. Few countries have adapted their legislation to accommodate electronic evidence. However, the majority relies on old laws and applies them to electronic evidence by analogy. There are thus significant differences in national legislation and approaches, which makes the handling of electronic evidence difficult across jurisdictions. In all cases, the legislation requires a clear scope of application of powers and sufficient legal authority for actions, but the conditions may vary considerably even in countries with the same legal tradition. Albeit, a number of international and international and European legal instruments and policy documents are, in principle, relevant to electronic evidence, including EU legal initiatives and guidelines, and the legal instruments and documents by the Council of Europe. On the other hand, the legal regime concerning the exchange and transfer of electronic evidence is more elaborative and at the moment, under intense reform. Due to its high importance for electronic evidence, this framework will be studied separately in Section 5.

3.1 European Union

3.1.1 Primary law

Even though with the adoption and entry into force of the Lisbon Treaty, a supranational regime for EU criminal law was established, judicial and police cooperation including the handling of evidence, are subject to Article 4(2) of the Treaty on the European Union (TEU). According to this Article, national security is the sole responsibility of the Member States, emphasising on the notion of state sovereignty.

Law enforcement access to personal data, such as subscriber information,[70] metadata and content data, may constitute an interference with the right to privacy, guaranteed under Article 7 of the EU Charter of Fundamental Rights and Freedoms, and with the right to the protection of personal data, guaranteed under Article 8.[71] Article 52(1) of the Charter states that limitations on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and must respect the essence of these rights and freedoms.[72] As discussed in detail in D3.1 in the sections concerning proportionality, limitations may be imposed on these rights and freedoms under the condition that they are necessary and genuinely meet objectives of general interest recognised by the European Union[73] or protection of the rights and freedoms of others.[74] The possibility for the Member States to impose limitations on the rights to data protection and privacy are provided for by EU law.[75]

[69] EVIDENCE project (2016), European Informatics Data Exchange Framework for Courts and Evidence, D3.1 Overview of existing legal framework in the EU Member States.
[70] Including traffic data, location data and access logs.
[71] Statement of the Article 29 Working Party, Data protection and privacy aspects of cross-border access to electronic evidence, Brussels, 29 November 2017.
[72] Ibid.
[73] CJEU, Judgment Arkady Romanovich Rotenberg v. Council of the European Union, T-720/14.
[74] Ibid.
[75] Ibid.

3.1.2 Secondary law

Currently, the following secondary legal instruments are applied to matters relating to electronic evidence in EU. Even though most of these instruments are dealing with the topic of cross-border police and judicial cooperation, they may include some general principles and guidelines concerning the handling of evidence, and in particular electronic evidence, by the Member States:[76]

- The European Investigation Order (EIO) Directive,[77] which came into force in May 2017, sets up a new system that aims to allow the EU Member States to obtain evidence from other Member States involved in criminal cases with a cross-border element, in a faster and simplified way. For it is the main instrument governing the police and judicial cooperation concerning investigation orders in cross-border cases, it will be further discussed in the dedicated section.
- The Regulation (EU) 910/2014 (so-called eIDAS) of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.[78] The Regulation ensured that electronic files are admissible as evidence in legal proceedings and that will not be denied legal admissibility solely on the grounds of their electronic form.
- The 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.[79]

Although it is neither an instrument of secondary law nor a binding document, the European Union Agency for Network and Information Security (ENISA) Handbook and Guide[80] outlines a number of guiding principles for national law enforcement authorities and Computer Emergency Response Teams (CERTs), when collecting and handling evidence, and specifically electronic evidence.

3.1.2.1 GDPR and Directive 2016/680

The General Data Protection Regulation applicable as from 25 May 2018 and the Directive 2016/680[81] for the processing of personal data in the law enforcement context was discussed in detail in D3.1. Article 2 paragraph 2. lit (d) of the General Data Protection Regulation states that the Regulation shall not be applicable to personal data processing "by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the

[76] EVIDENCE project, European Informatics Data Exchange Framework for Courts and Evidence, D3.1 Overview of existing legal framework in the EU Member States.
[77] 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.
[78] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257/73.
[79] 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, p. 8–14.
[80] ENISA, Electronic evidence - a basic guide for First Responders Good practice material for CERT first responders [2014]; ENISA, Identification and handling of electronic evidence –Handbook, document for teachers [2013] September 2013.
[81] 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.

execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".[82] The General Data Protection Regulation, therefore, is not applicable to the collection and exchange of electronic evidence in this context. This type of processing is covered by the Directive 2016/680 in the manner it was transposed in the domestic law. Member States are also permitted to adopt national measures that restrict "the rights of data subjects when such measures are necessary and proportionate in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned".[83]

The Directive 2016/680 does not contain any specific rules on surveillance or any rules on innovative methods and technologies of gathering electronic evidence, such as retrieving data from cloud storages, interception of communications prior to encryption through software on terminal devices, and so forth. As a result, the Directive does not provide for adequate safeguards in this particular field. This *lacuna* could be argued that it is covered by the general principles of the GDPR, interpreted with the flexibility necessary in the law enforcement context.[84]

3.1.2.2 E-privacy reform

In 2017 the Commission adopted its proposal for a new ePrivacy Regulation concerning the protection of personal data in electronic communications to repeal Directive 2002/58/EC and to modernise privacy law regarding telecommunications by adjusting to the GDPR principles. This Regulation will particularise and complement the GDPR[85] by laying down specific rules. The relation to the Directive 2016/680/EU is not stated specifically. However, it is indirectly concluded by the GDPR recital (19): "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, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council".

A "competent authority" can be a private entity as well, but only if exercising public authority on a Member State's behalf. Any collection or storing of electronic evidence stemming from telecommunications networks by the service provider or any private entity, will not fall under Directive 2016/680/EU since service providers are not entrusted with public powers.[86] For instance, any future data retention will fall under the new ePrivacy regulation. If, however, LEAs get involved, the situation becomes more complex. According to the Court of Justice of the EU (CJEU) in reference to the Directive 2002/58/EC, the access to telecommunications data by public authorities falls into

[82] Statement of the Article 29 Working Party, Data protection and privacy aspects of cross-border access to electronic evidence, Brussels, 29 November 2017.
[83] Ibid.
[84] Ibid.
[85] Article 1(3) GDPR.
[86] COMMISSION STAFF WORKING DOCUMENT, Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC, Accompanying the document - Proposal for a Regulation of the European Parliament and the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, Brussels, 10.1.2017, SWD(2017) 5 final.

the scope of the Directive 2016/680 when this data was collected by private entities in compliance with a law aiming at the use of such data for criminal investigation.[87]

Thus, access to such data by public authorities concerns the processing by telecommunications providers and therefore falls into the scope of the Directive 2002/58/EC. The situation is different if LEAs lawfully intercept telecommunications data themselves. Then the Directive 2016/680 would be applicable. Accordingly, the material scope of the draft ePrivacy Regulation explicitly excludes "activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security",[88] leaving Directive 2016/680/EU solely applicable for all cases, in which electronic evidence is collected by competent authorities from telecommunications networks.[89]

3.2 Council of Europe

Regarding electronic evidence, Council of Europe (CoE) has adopted instruments and documents that are highly relevant:[90]

- The European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) in particular concerning the protection of the rights to privacy and due process;
- The Council of Europe Convention on Cybercrime (or the so-called Budapest Convention or CoE Cybercrime Convention), as this Convention remains the main and only international treaty which defines the substantive elements of cybercrime, as seen in D3.1. This Convention also establishes the main framework for reference in the area of electronic evidence since it offers many provisions to enable investigations in cases where electronic evidence is involved.[91]
- The Council of Europe Convention on Mutual Assistance in Criminal Matters, which entered into force in 1962, and its 1978 Protocol. However, it does not include specific provisions for electronic evidence;[92]
- The Council of Europe Recommendation 87 (15) regulating the use of personal data in the police sector.[93]
- The Electronic Evidence Guide, although non-binding, also offers guidance for Law Enforcement Agencies;[94]

3.2.1 The European Convention on Human Rights and the case law of the Strasbourg Court

The European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and its Protocols have been signed and ratified by all the EU Member States. The right to liberty

[87] Biasiotti, M. (2018).
[88] Recital 19 of the GDPR:
[89] Ibid.
[90] EVIDENCE project, European Informatics Data Exchange Framework for Courts and Evidence, D3.1 Overview of existing legal framework in the EU Member States.
[91] Ibid.
[92] Council of Europe, European Convention on Mutual Assistance in Criminal Matters, ETS No.030, Strasbourg 12 June 1962.
[93] Council of Europe, Recommendation No. R (87) 15, 17 September 1987.
[94] Council of Europe, Data protection and Cybercrime Division, Electronic Evidence Guide, Strasbourg 3 February 2013.

(Art.5 ECHR), the right to a fair trial (Art.6 ECHR) and the right to private and family life (Art. 8 ECHR) have a profound influence on criminal proceedings, including obtaining and handling evidence. In particular, the right to a fair trial guarantees a set of minimum rights, including the right to a public trial within a reasonable time by an independent and impartial court established by law, and the presumption of innocence. It also includes the right to remain silent and not incriminate oneself, the right to have the resources to prepare one's defence, the right to be informed of the charges, the right to examine witnesses, the right to be assisted by a counsel and/or by an interpreter, if necessary.[95] The rights guaranteed by Article 6 of the Convention can be exercised by the defendant or by his/her counsel.

The right to a fair trial applies to the court proceedings but also to the investigations, and thus, the fairness must be assessed in light of the whole process.[96] In its case-law, the ECtHR constantly reiterated that Article 6 of the Convention does not require the adoption of evidence rules since that is an issue to be dealt with in the domestic law.[97] "[T]he admissibility of evidence is primarily a matter for regulation by national law, and as a general rule, it is for the national courts to assess the evidence before them".[98] The Court, under Article 6, is to make sure that the legal proceedings as a whole, including the manner evidence, was obtained and handled by all competent authorities, were fair.[99] The domestic law, on the other hand, defines what types of evidence are admissible and relevant, what the probative value of the evidence is, and how evidence should be evaluated.[100] Such an approach is considered inevitable given the wide variations in the law of evidence in the different European legal systems.

Nevertheless, the right to a fair trial also implies the right for the defendant to challenge the reliability of the evidence brought against him/her and to oppose its admissibility.[101] The ECtHR is only competent to deal with errors of facts or law allegedly committed by domestic courts in violation of rights and freedoms safeguarded in the Convention. The Court held that "insofar the statements of a usual witness, of a civil party, of an injured party, of a police informant or an expert, are used to found a conviction, all these statements are evidence" which fall under the protection of Article 6 (1) and (3).[102] In other words, where a statement or report may be the basis for a conviction, then it constitutes evidence for the prosecution.[103] As established by the interpretation of Article 6 (3) (d), in principle, the evidence must be produced in the presence of the accused with the possibility of an adversarial argument at a public hearing.[104] The accused must be given "an

[95] Vuille, J. et al. (2017), Scientific evidence and the right to a fair trial under Article 6 ECHR, Law, Probability and Risk, Volume 16, Issue 1, 1 March 2017, pp. 55–68.
[96] Ibid.
[97] European Judicial Training Network (EJTN), Evidence And Proofs From The Perspective Of The European Court of Human Rights, *ejtn.eu*
[98] ECtHR, judgment of 9 June 1998, Teixeira de Castro v Portugal, appl. no. 25829/94.
[99] Ibid.
[100] European Judicial Training Network (EJTN), Evidence And Proofs From The Perspective Of The European Court of Human Rights, *ejtn.eu*
[101] Vuille, J. et al. (2017).
[102] ECtHR, judgment of 22 April 1992, Vidal v. Belgium, para 33.
[103] European Judicial Training Network (EJTN), Evidence And Proofs From The Perspective Of The European Court of Human Rights, *ejtn.eu*
[104] Summers, S. (2007), Fair Trials - The European Criminal Procedural Tradition and the European Court of Human Rights, Hart Publishing.

adequate and proper opportunity to challenge and question a witness against him/her". When a conviction is exclusively based on a statement taken at the proceedings during the pre-trial stage, and the accused had no opportunity to challenge and question the witness, then this could amount to a violation of Article 6. Statements not made in court, but to other authorities, shall be viewed as statements of witness insofar as the national courts consider these statements.[105]

Specifically, when expert evidence, be that conventional or digital forensics expertise, is adduced, the right to a fair trial requires that equality of arms be upheld between the parties: whenever a prosecution expert is commissioned, the defendant must be allowed his/her own expert; and whenever a court-appointed expert is commissioned, he/she must be impartial and neutral.[106] Moreover, the parties must have a right to participate in the expert's examination meaning that the parties must have an opportunity to comment, make observations and request a further investigation on the expert's findings; in particular when the topic is of technical nature. Expert evidence of favourable nature must be communicated to the defendant and must be accounted for in the proceedings. The defendant must also be given the opportunity to confront the expert. Even in a non-adversarial setting, this implies that the court must hear the expert at the trial stage if it is going to base its conviction mainly on the expert's report.

Evidence that may be relevant can be excluded as a matter of law discretion because it is was obtained illegally, improperly or unfairly.[107] The use of evidence obtained illegally under national law is not, in itself, a breach of the right to a fair trial, except for the unacceptability of evidence obtained by entrapment. Nevertheless, the defence must be given the opportunity to challenge the use and authenticity of the evidentiary material, and other evidence should also be brought in support of the conviction. If no doubts arise as to its authenticity, then the Court will check whether the rights of the defendant have been fully respected alongside with the probative value of the evidentiary material.[108] Nonetheless, use of unlawful methods to obtain evidence should be condemned as a preliminary matter.[109]

Moreover, the right to fair trial can be read in conjunction with Articles 2 and 3, wherever the conviction was found on evidence obtained in breach of Article 3 of the Convention. The Strasbourg Court in those cases held that the examination of the fairness of the procedure presupposes examination of the quality of the evidence and the circumstances in which it was obtained. The Court did not exclude that on the facts of a particular case the use of evidence obtained by an act qualified as inhuman and degrading treatment not amounting to torture "will render the trial against the victim unfair, irrespective of the seriousness of the offence allegedly committed, the weight attached to the evidence and the opportunities which the victim had to challenge its admission and use at his trial".[110] The Court has reaffirmed that "even in the most

[105] ECtHR, judgment of 19 February 1991, Isgrò v. Italy, appl.no. 11339/85, para 12.
[106] European Judicial Training Network (EJTN), Evidence And Proofs From The Perspective Of The European Court of Human Rights, *ejtn.eu*
[107] Keane, A. (2008), The Modern Law of Evidence, Oxford University Press, p. 53.
[108] European Judicial Training Network (EJTN), Evidence And Proofs From The Perspective Of The European Court of Human Rights, *ejtn.eu*
[109] ECtHR, judgment of 19 June 2003, Hulki Güneş v. Turkey, appl.no. 28490/95.
[110] European Judicial Training Network (EJTN), Evidence And Proofs From The Perspective Of The European Court of Human Rights, *ejtn.eu*

difficult circumstances, such as the fight against terrorism and organised crime, the Convention prohibits in absolute terms torture and inhuman or degrading treatment or punishment, irrespective of the conduct of the person concerned". It, however, considered that the criminal trial's fairness was only at stake if the evidence obtained in breach of Article 3 was decisive for the defendant's conviction. A national court must always make a thorough assessment as to whether the means by which particular evidence has been obtained would render unfair its use in the trial.[111]

3.2.2 The Cybercrime Convention

As already seen in D3.1, the key aim of the Cybercrime Convention is to harmonise domestic criminal substantive law in the area of cybercrime, provide for powers necessary for the investigation and prosecution of cybercrime as well as other offences committed with the means or against a computer system, by regulating electronic evidence and establishing a fast and effective regime of international cooperation.

3.2.2.1 Jurisdiction

Jurisdiction is the power of a state under international law to regulate its affairs and reflects the principles of state sovereignty as well as equality among states and non-interference in domestic affairs. Electronic evidence, due to its nature, may be stored or located in another jurisdiction than the one where the crime was committed. Jurisdiction in cybercrime cases thus is both executive – the capacity of a state to act inside another state - and judicial – the capacity of the Court of a state to try cases with a foreign element. In Article 22, therefore, the Cybercrime Convention relies on the principle of territoriality, which entails the jurisdiction of a state over its nationals in order to establish jurisdiction for cybercrime.

Article 22 of the CoE Cybercrime Convention – Jurisdiction

1. *Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention when the offence is committed:*

a. *in its territory; or*
b. *on board a ship flying the flag of that Party; or*
c. *on board an aircraft registered under the laws of that Party; or*
d. *by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.*

[…]

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

3.2.2.2 Investigative powers

When it comes to the investigation in cybercrime cases and the extraction of electronic evidence, enforcement authorities may need a variety of powers to collect, preserve and exchange electronic

[111] McBride, J., The case law of the European Court of Human Rights on evidentiary standards in criminal proceedings, European Union - Council of Europe joint project "Application of the European Convention on Human Rights and harmonisation of national legislation and judicial practice in line with European standards in Georgia".

evidence. They might need traditional but also cyber-specific powers.[112] Evidence may come in the form of computer files, logs, transmissions, metadata, computer data and what not. As previously stated, there are significant differences between the different national enforcement legislations and approaches. In certain countries traditional investigative powers may be general enough to apply to cybercrime cases while in other states the conventional procedural law may not apply to cyber-specific issues, making additional cyber-specific legislation necessary.[113] The main gaps in investigative powers include the lack of power to enter electronic networks in order to search for evidence and preserve computer data to support existing search powers.[114] Nevertheless, the Cybercrime Convention provides for a set of minimum investigative powers that States may adopt.

Article 14 of the CoE Cybercrime Convention – Scope of procedural provisions

1. *Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings*
2. *Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:*
   a. *the criminal offences established in accordance with Articles 2 through 11 of this Convention;*
   b. *other criminal offences committed by means of a computer system; and*
   c. *the collection of evidence in electronic form of a criminal offence.*

[…]

The Article 14 of the Cybercrime Convention provides that the States Parties to the Convention shall adopt legislation and other measures that establish powers and procedures for criminal investigations and proceedings for the offences referred to in the Convention and for the collection of electronic evidence. Since such evidence can be altered easily, the admissibility of the evidence may be at stake.[115] Therefore, when gathering and handling electronic evidence, the integrity, authenticity and continuity of such evidence must be guaranteed during the entire chain of custody until trial.[116] While some states still apply traditional evidential rules to electronic evidence by analogy, other states already have special rules for electronic evidence. The procedural aspects in the Cybercrime Convention empowering the competent authorities in the States Parties include: expedited preservation of stored computer data and traffic data (Art. 16 and Art. 17), the

[112] Article 29 Data Protection Working Party, Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime, adopted on 22 March 2001, 5001/01/EN/Final WP 41.
[113] Biasiotti, M. et al (2018).
[114] Ibid.
[115] Cristina Schulman, Legislation and legal frameworks on cybercrime and electronic evidence: Some comments on developments 2013 – 2018, United Nations Intergovernmental Expert Group on Cybercrime, Panel on legislation and legal frameworks, Vienna 3-5 April 2018.
[116] EVIDENCE project, European Informatics Data Exchange Framework for Courts and Evidence, D3.1 Overview of existing legal framework in the EU Member States.

production order (Art. 18), search and seizure of stored computer data (Art. 19), real-time collection of traffic data (Art. 20) and interception of content data (Art. 21).[117]

All investigative powers are subject to the conditions and safeguards under Art. 15 of the Convention, meaning that they are to be executed in accordance with individual rights and freedoms, the principle of proportionality, judicial or other independent oversight, legal ground, restricted scope and limited duration for the application of any measure.[118] Nevertheless, the Cybercrime Convention is a Council of Europe Convention,[119] which means that it is not a European Union instrument, and as such, it is open to non-European Union states. Those states, in contrast with the EU Member States, are not required to be parties to the European Convention on Human Rights, or to the Council of Europe Convention No. 108 for the processing of personal data.[120] This observation entails that some non-EU states may not have in place the same safeguards and level of protection for human rights. The T-CY Cloud Evidence Group's report on Criminal justice access to data in the cloud states that "[i]t is presumed that the Parties to the Convention form a community of trust and that rule of law and human rights principles are respected in line with Article 15 Budapest Convention."[121] Article 15 only requires compliance with human rights requirements in relation to "the establishment, implementation and application of the powers and procedures provided for in", which relates to procedural law. It neither ensures nor requires that Parties comply with international human rights standards in relation to any substantive criminal law. Moreover, the Convention does not clarify how Article 15 is to be applied by State Parties.[122]

Article 15 of the CoE Cybercrime Convention — Conditions and safeguards

1. *Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.*
2. *Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.*
3. *To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.*

[117] Cristina Schulman, Legislation and legal frameworks on cybercrime and electronic evidence: Some comments on developments 2013 – 2018, United Nations Intergovernmental Expert Group on Cybercrime, Panel on legislation and legal frameworks, Vienna 3-5 April 2018.
[118] Forgó, N., et al. (2018), Privacy Protection in Exchanging Electronic Evidence in Europe, in: Handling and Exchanging Electronic Evidence Across Europe, pp. 255–288.
[119] EDRi, Cybercrime Convention -cross-border access to electronic evidence, 17 January 2017.
[120] Ibid.
[121] Ibid.
[122] Ibid.

Expedited preservation of stored computer data, as described in Article 16 of the Cybercrime Convention is a provisional measure that allows competent authorities to order immediate preservation of stored data that is held by a third party which may be a service provider, a natural or a legal person, for up to 90 days. Such a power allows competent authorities to gain some time in order to obtain the right authorisation before exercising additional investigative powers, without risking the integrity or loss of the evidentiary material. The preservation order may be subsequently renewed and the third party preserving the computer data may be obliged to keep confidential the undertaking of the procedures for the period of time provided for by national law.[123]

If the data to be preserved under the expedited preservation order within the previous paragraph is considered to be traffic data, measures may be taken to ensure that such preservation is available regardless of whether one or more service providers were involved in the transmission of that communication and despite the shorter retention periods of such data.[124] This provision is deemed necessary in order to allow the competent authorities to detect and identify the parties involved in the case. Article 17 provides for the competent authority to issue preservation orders to more service providers, if it is deemed necessary for the disclosure of sufficient traffic data.

Article 16 of the CoE Cybercrime Convention – Expedited preservation of stored computer data

1. *Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.*
2. *Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.*
3. *Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.*
   [...]

Article 17 of the CoE Cybercrime Convention – Expedited preservation and partial disclosure of traffic data

1. *Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:*
   a. *ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and*
   b. *ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party*

[123] Council of Europe, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, CETS 185, para 162 and 163.
[124] Ibid, para 161.

> *to identify the service providers and the path through which the communication was transmitted.*
>
> *[…]*

Based on Article 18 of the Convention,[125] competent authorities may order persons in their territory to submit computer data that is in that person's possession or control. The data may be stored in a computer system or in a storage medium. Moreover, the competent authorities may order a service provider offering its services in the territory of the State where the competent authority is located to submit subscriber information which is related to its services and is in the service provider's possession or control.[126]

The term "subscriber" is an umbrella term for a wide spectrum of service provider clients, including individuals with paid subscriptions, users who pay on a per use-basis as well as free services users. It might also include information concerning persons who are entitled to use the subscriber's account, for instance, family members.[127] Any information, in the form of computer data or any other form held by a service provider, relating to subscribers of its services other than traffic or content data, directly or indirectly pertaining to the use of the communication service and by which various details relating to the service and the subscriber can be established, may be considered as subscriber information.[128] As subscriber information seems to be less privacy sensitive than traffic data and content data, conditions for production orders for subscriber information can be subject to lesser safeguards than for other types of data or for other types of intrusive powers, in order to facilitate domestic investigations and international cooperation in a cloud context, for example.[129]

According to Article 18 of the Cybercrime Convention, the production of subscriber information could, therefore, be ordered under two circumstances: first, if the criminal justice authority has jurisdiction over the alleged offence and second if the service provider is in possession or control of the subscriber information.[130] Two more conditions have to be met: a. either the person is in the territory of the Party or b. the service provider is "offering its services in the territory of the Party". Relevant factors that will be taken into account to assess whether or not a provider offers its services in the territory of a State Party include, for example, local advertising.[131] Moreover, the provider must use the subscriber information and other associated traffic data in the course of its activities and must actively interacts with subscribers in the State Party. In other words,

[125] Council of Europe, Cybercrime Convention Committee (T-CY), T-CY Guidance Note #10, Production orders for subscriber information (Article 18 Budapest Convention), Strasbourg 1 March 2017, T-CY (2015)16.
[126] Ibid.
[127] Ibid, p.8.
[128] Palmer, A. (2018), Mutual Legal Assistance: Understanding the Challenges for Law Enforcement in Global Cybercrime Cases, Center for Cyber and Homeland Security, The George Washington University, Issue Brief – January 2018.
[129] Council of Europe, Cybercrime Convention Committee (T-CY), Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final report of the T-CY Cloud Evidence Group, Strasbourg France, 16 September 2016, p.38.
[130] Council of Europe, Cybercrime Convention Committee (T-CY), T-CY Guidance Note #10, Production orders for subscriber information (Article 18 Budapest Convention), Strasbourg 1 March 2017, T-CY (2015)16, p.9.
[131] Ibid.

the criteria used are similar to assess whether a provider is considered to be established in the territory of a State Party.[132]

Article 18 of the CoE Cybercrime Convention – Production order

1. *Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:*
   a. *a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and*
   b. *a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.*

   […]

According to Article 19 of the Convention, the competent authorities may search or access a computer system and computer data stored therein as well as a computer storage medium in which computer data may be stored in the territory of the state where the competent authority is located. This search may be extended, if deemed necessary, to another computer system within the territory of the state where the competent authority is located.[133]

Article 19 of the CoE Cybercrime Convention – Search and seizure of stored computer data

1. *Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:*
   a. *a computer system or part of it and computer data stored therein; and*
   b. *a computer-data storage medium in which computer data may be stored in its territory.*

   […]
3. *Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:*
   a. *seize or similarly secure a computer system or part of it or a computer-data storage medium;*
   b. *make and retain a copy of those computer data;*
   c. *maintain the integrity of the relevant stored computer data;*
   d. *render inaccessible or remove those computer data in the accessed computer system.*

   […]

According to Article 20 of the Convention, competent authorities have the power to collect or record traffic data transmitted by a computer system by technical means in real-time. The competent authority can oblige a service provider to collect or record or to cooperate with and assist the competent authorities in the collection or recording of traffic data, since such data is

[132] Council of Europe, Cybercrime Convention Committee (T-CY), T-CY Guidance Note #10, Production orders for subscriber information (Article 18 Budapest Convention), Strasbourg 1 March 2017, T-CY (2015)16.
[133] Council of Europe, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, CETS 185, para 193, 194 and 195.

crucial for tracing a communication back to a perpetrator.[134] The collection or recording should be related to traffic data of specified multiple communications and within the territory of the state where the competent authority is located.[135] The confidentiality obligation applies in this case too.[136]

Article 20 of the CoE Cybercrime Convention – Real-time collection of traffic data

1. *Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:*
   - *a- collect or record through the application of technical means on the territory of that Party, and*
   - *b- compel a service provider, within its existing technical capability:*
     - *i. to collect or record through the application of technical means on the territory of that Party; or*
     - *ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system*

   […]

Like in the case of collection of traffic data, the competent authorities may further be granted the power to intercept content data, in real-time and by technical means within the territory of the State where the competent authority is located, in relation to a range of serious offences to be determined by national law. Nevertheless, interception of content data, i.e. the communication content is more intrusive and thus it is allowed only in case of a serious offence.[137] The competent authority may further compel a service provider to collect or record, cooperate and assist with the collection or recording of content data.[138]

Article 21 – Interception of content data

1. *Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:*
   - *a. collect or record through the application of technical means on the territory of that Party, and*
   - *b. compel a service provider, within its existing technical capability:*
     - *i. to collect or record through the application of technical means on the territory of that Party, or*
     - *ii. to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.*

   […]

[134] Ibid, para 220.
[135] Ibid, para 219.
[136] Ibid, para 225 and 226.
[137] Ibid, para 229.
[138] Ibid, para 230.

Last but not least, according to Art. 32 (a) of the Cybercrime Convention a state may unilaterally access publicly available computer data, regardless of where the data is located, without seeking mutual assistance.[139] Moreover, Art. 32 (b) establishes the direct voluntary disclosure, if the person who has the lawful authority to disclose the data provides their consent.[140] [141] It may be for example a person's e-mail communications stored in another jurisdiction by the service provider.[142] Even though voluntary disclosure is allowed, hacking back with the intention to deploy electronic countermeasures in order to track down and disable offenders´ computers and devices may in itself be an illegal act, which is not explicitly regulated in the Convention and should be considered in a national basis.

3.2.3 The CoE Recommendation 87 (15)

The CoE Recommendation contains several principles both on the collection and on the transfer of personal data in the police sector and therefore covers electronic evidence. Even though it dates back to 1987, Recommendation 87 (15) has proven quite visionary in many regards and has influenced many subsequent legal acts of the CoE and the EU.[143] The following list gives an overview of those principles, which can be considered relevant to electronic evidence.[144]

Principle 1—Control and notification
[...]
1.2. New technical means for data processing may only be introduced if all reasonable measures have been taken to ensure that their use complies with the spirit of existing data protection legislation.
1.3. The responsible body should consult the supervisory authority in advance in any case where the introduction of automatic processing methods raises questions about the application of this recommendation.
[...]

Principle 2—Collection of data
2.1. The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation.
[...]
2.3. The collection of data by technical surveillance or other automated means should be provided for in specific provisions.
2.4. The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not prescribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry.

Principle 3—Storage of data
[...]

[139] Ibid, para 293.
[140] Council of Europe, Cybercrime Convention Committee (T-CY), T-CY Guidance Note #3 Transborder access to data (Article 32), Strasbourg, 3 December 2014.
[141] Vatis, M. A. (2010), The Council of Europe Convention on Cybercrime, in: Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.
[142] Ibid.
[143] Forgó, N., et al. (2018), p. 275.
[144] Ibid.

3.2. As far as possible, the different categories of data stored should be distinguished in accordance with their degree of accuracy or reliability and, in particular, data based on facts should be distinguished from data based on opinions or personal assessments.
3.3. Where data which have been collected for administrative purposes are to be stored permanently, they should be stored in a separate file. In any case, measures should be taken so that administrative data are not subject to rules applicable to police data.
[...]

5.5.i. Requests for communication
[...]
5.5.ii. Conditions for communication
As far as possible, the quality of data should be verified at the latest at the time of their communication. As far as possible, in all communications of data, judicial decisions, as well as decisions not to prosecute, should be indicated and data based on opinions or personal assessments checked at source before being communicated and their degree of accuracy or reliability indicated. If it is discovered that the data are no longer accurate and up to date, they should not be communicated. If data which are no longer accurate or up to date have been communicated, the communicating body should inform as far as possible all the recipients of the data of their non-conformity.

5.5.iii. Safeguards for communication
The data communicated to other public bodies, private parties and foreign authorities should not be used for purposes other than those specified in the request for communication. Use of the data for other purposes should, without prejudice to paragraphs 5.2 to 5.4 of this principle, be made subject to the agreement of the communicating body.

5.6. Interconnection of files and on-fine access to files
The interconnection of files with files held for different purposes is subject to either of the following conditions:
a. the grant of an authorisation by the supervisory body for the purposes of an inquiry into a particular offence, or
b. in compliance with a clear legal provision.
Direct access/on-line access to a file should only be allowed if it is in accordance with domestic legislation, which should take account of Principles 3 to 6 of this recommendation.

3.3 Common Principles of handling electronic evidence

Despite all the differences at national level regarding admissibility of electronic evidence, according to the extensive study funded by the European Union and the Council of Europe leading to the creation of the Electronic Evidence Guide and the ENISA´s Handbook on Digital Forensics, proper handling of any evidence, including electronic and more specifically digital evidence, requires following some general guidelines.[145]

3.3.1 The principle of data integrity

The first principle is data integrity. Handling electronic devices and data must not cause alterations either to software or hardware. The persons in charge of the investigation must assure the integrity of the evidentiary material by initiating a forensic chain of custody. Chain of custody or evidence refers to "the detailed documentation of the status of potential digital evidence at every point of time from the moment of collection, acquisition or seizure of the evidence to the moment the

[145] European Union Agency for Network and Information Security (ENISA), Identification and handling of electronic evidence –Handbook, document for teachers, September 2013.

evidence is presented in court."[146] When data on a live computer system or network must be assessed, in order to avoid the loss of potential evidence, the material must be collected by an expert with the right authorisation, causing the least impact on the data.[147]

3.3.2 The principle of audit trail

All actions from the first moment of collection until the presentation of the evidentiary material before the court should be recorded in a way that if an independent third party repeats those actions in the same exact manner, it will come to the same result. Only this way, the probative value of the evidence may be guaranteed.[148]

3.3.3 The principle of specialist support

For investigations involving search and collection of electronic evidence, the consultancy with external experts may be necessary. All external experts should be familiar with the general principles, as well as the rules and principles of the specific country where the legal proceedings take place.[149] The expert should have the necessary specialist expertise and experience in the field, investigative knowledge, knowledge of the matter at hand, legal knowledge, appropriate communication and language skills for both oral and written explanations and last but not least, appropriate authorisation for his/her involvement in the activities.

3.3.4 The principle of appropriate training

If no specialist support is available or if it is not necessary, first responders and electronic evidence examiners must be appropriately trained to search for and seize electronic evidence and to explain the relevance and implications of their actions in each specific case.[150]

3.3.5 The principle of legality

The persons and agencies in charge of the investigations are responsible for ensuring that the law, the general forensic and procedural principles, and all the above-listed principles are adhered to with regards to the possession of and access to electronic evidence.[151] Each Member State should take its legal documents and regulations into consideration when interpreting the principles proposed.[152]

[146] European Anti-Fraud Office (OLAF), Guidelines On Digital Forensic Procedures For OLAF Staff, 15 February 2016, p.1.
[147] European Union Agency for Network and Information Security (ENISA), Identification and handling of electronic evidence –Handbook, document for teachers, September 2013, p.4-6.
[148] Ibid.
[149] Ibid.
[150] Ibid.
[151] Ibid.
[152] Ibid.

4. Electronic evidence: national frameworks

4.1 National frameworks of relevance for CYBER-TRUST

Even though it is not possible to refer to a pan-European approach, there is a number of principles and good practices which seem to apply in most jurisdictions, as seen above.[153] In many jurisdictions, electronic evidence is equivalent to traditional evidence, for instance, either in the form of electronic documents (equivalent to paper documents), or electronic signatures (equivalent to hand-written signature), or electronic communications (equivalent to postal correspondence).[154] Other jurisdicitons have adopted explicit laws concerning electronic evidence. In both cases, it is of paramount importance that the persons in charge of handling electronic evidence prior to their examination by competent authorities, treat it in such a manner that any recovered data will have a good chance to be admissible as evidence in later proceedings.[155] Nevertheless, the law of evidence is primarily a domestic matter. Here follows, therefore, the description of the relevant legislation in countries of relevance for CYBER-TRUST.[156]

4.1.1 Cyprus

The Law of Evidence, Chapter 9 is the main legal instrument in Cyprus, as amended with the Law 32(I)/2004.[157] Pursuant to the Article 3 of the Law of Evidence, the Cypriot Courts without prejudice to the provisions of the present law must implement the Law and the rules of evidence of the United Kingdom as of 5 November 1914. [158] Other relevant laws are: a. the Law for the organisation of the Courts n.14/60, b. the Criminal Code, Chapter 154, and c. the Law for the Interpretation, Chapter 1. All three laws concern the interpretation and implementation of the criminal law in accordance with the Cypriot Constitution, the common law principles and the relevant UK legislation. Police authorities have the following investigative powers under national law, as already seen in D3.1:[159] a. search and seizure of information systems/computer data (Code of Criminal Procedure); b. preservation of computer data (Law 22(III)/2004 – this is the Law ratifying the CoE Cybercrime Convention); c. order for stored traffic/content data, however, only for stored traffic data (Law 183(I)/2007); d. order for user information (Law 183(I)/2007). Nevertheless, real-time interception/collection of traffic/content data is not permitted. The Law 183(I)/2007 forces ISPs to store telecommunication and traffic data for the purpose of investigation for a period of six months. The chain of custody must be fully documented, based according to the Police Order 3/17 and the Forensic Lab Manual.[160]

[153] Ingle, J. (2014); Jackson, J. and Summers, S. (2012).
[154] Insa, F. (2007).
[155] Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, March 2012.
[156] This Section is based on the preliminary findings of CYBER-TRUST, D3.1 Regulatory Framework Analysis.
[157] The text of the Law can be found here: http://www.cylaw.org/nomoi/enop/non-ind/0_9/full.html
[158] Information about the legal framework in Cyprus, available at: http://www.law.gov.cy/law/lawoffice.nsf/dmltestgeneral_gr/dmltestgeneral_gr?OpenDocument
[159] Council of the European Union, Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating Cybercrime" - Report on Cyprus, Brussels, 15 July 2016, 9892/1/16 REV 1, p.38.
[160] Council of the European Union, Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating Cybercrime" - Report on Cyprus, Brussels, 15 July 2016, 9892/1/16 REV 1, p.38.

Evidence which is acquired in violation of the constitutional rights of an individual is not admitted in criminal proceedings, and this rule leaves no room for exceptions, in particular with regards to the protection of private life and the confidentiality of communications.[161] Admission of evidence obtained in breach of fundamental rights would be incongruous with the efficient application of the provisions of the Constitution, in particular, the right to fair trail. Thus there is no discretion for the Court to admit evidence obtained or secured by contravention of the fundamental rights and liberties safeguarded by the Constitution and the European Convention on Human Rights.[162] Concerning the confidentiality of communications, some exceptions apply only for the investigation of very serious crime and only pursuant to the safeguards of the specific laws.[163] Moreover, other Cypriot Courts have called inadmissible evidence in electronic form, which contained a copy of emails and other computer data, despite the fact that the competent authorities were authorised for the search and seizure. In both cases, the defendant did not freely consent that the police becomes the recipient of their confidential communication files.[164] In other cases, evidence, including disks, copies of disks, computers, etc. was considered inadmissible, and all subsequent police acts illegitimate because the gathered evidence contained material taken from the internet and constituted communication between the electronic address of the defendant and the electronic address of the website.[165]

4.1.2 Greece

As discussed in D3.1, the Greek Code of Criminal Procedure is the primary piece of legislation pertaining to rules of evidence.[166] Article 177 establishes the principle of "moral proof" stricto sensu or the free judgment of the evidentiary material. Every lawfully acquired evidence is in principle admissible. Investigating authorities and Courts have a duty to search for the factual truth, being entitled to initiate any investigating act with respect to evidence considered necessary to reveal the truth. Means of proof can include indices, inspection of persons, places and objects, experts' reports, confessions, statements of witnesses and documents.[167]

Article 177 of the Greek Code of Criminal Procedure provides for the general inadmissibility of illegally obtained evidence. Nevertheless, it is often accepted that illegally obtained evidentiary material is admissible, if favourable for the defendant, only after weighing the conflicted interests and with regards to the principle of proportionality, as prescribed in the Greek Constitution. Moreover, Article 19 para 3 of the Greek Constitution introduces the absolute prohibition of the admissibility of evidence which was obtained in violation of the right to private life, data protection and confidentiality of communications, with the exemption of national security and prosecution of

[161] The Police v Georgiades (1982) 2 CLR 33, Supreme Court of Cyprus, p.43.
[162] The Police v. Georghiades (1983) 2 CLR 33.
[163] State v Panikou a.o. (1998) 1 ΑΑΔ.
[164] The Judgment is in accordance with the finding in the ECtHR, Copland v United Kingdom, Appl. No. 62617/00, that the confidentiality of communications covers the use of email services and the internet.
[165] *Αστυνομία v. Αλεξάνδρου (2010)* Αρ. Αγ. 729/07 Επαρχιακού Δικαστηρίου Λευκωσίας
[166] Quinn, P. (2016).
[167] This information can be found at the Greek Legal Digest Website, available at http://www.greeklawdigest.gr/topics/judicial-system/item/16-procedure-before-criminal-courts [Accessed: 02.08.2018].

very serious crime. The Hellenic Police is in charge of the process of collection, acquisition and preservation of the electronic evidence.

4.1.3 Italy

In Italy, the collection of electronic evidence is mainly regulated by the Italian Code of Criminal Procedure, as discussed as well in D3.1.[168] The inspection of persons, places and objects occurs only with the right authorisation and within the aim to ascertain the evidence of a crime.[169] The centerpiece in the field of digital forensics in Italy is the "electronic document", the digital representation of judicially relevant facts or events, based on Article 1(p) of Legislative Decree 82/05 (the so-called "Digital Administration Code").

Law no. 48 of 18 March 2008 (Law 48/2008) specified that, as far as electronic evidence is concerned in the provisions of the Code of Criminal Procedure, investigators, after the authorisation of a competent judicial authority, shall adopt "the technical measures aimed at ensuring the preservation of original data and preventing it from being altered".[170] [171]the Italian Electronic Communications Code, service operators are obliged to assist judicial authorities by providing "compulsory services", which include the delivery of data and interception of communications upon request.[172]

A "digital inspection" may be requested if there are reasonable grounds to believe that data, information or software of the prosecuted crime is to be found within an information system.[173] The specific material may be requested by the judicical authority to be delivered for further examination. If the owner of the object agrees to hand it in, an inspection may not be initiated. In all other cases, an inspection may be considered necessary. When a judicial order for the seizure of data from internet services or telecommunications providers is issued, including traffic and location data, in order to acquire the material, it may be deemed necessary to copy it on a suitable medium, ensuring the originality and non-alteration of it. Urgent inspection for the collection of evidence is also permitted in the case where there is imminent danger that the evidence will be altered or spoiled, and the judicial authority has not yet assumed the control of the proceedings.[174] In April 2016, following an Italian Court decision, the use of malware for the interception of information so as to investigate serious offences pertaining to organised crime and terrorism, "within private residences," without prior authorisation by a judicial authority, and even without high degree of certainty that a crime has been actually committed, was considered lawful.[175]

[168] Mitja, G., et al (eds.) (2014), The Italian Code of Criminal Procedure. Critical Essays and English Translation, CEDAM and Wolters Kluwer Italia.
[169] De Zan, T. and Autolitano, S. (2016), EUnited Against Crime: Improving Criminal Justice in European Union Cyberspace, Instituto Affari Internazionali, p.48.
[170] Italy - Country Wiki - Council Of Europe, https://www.coe.int/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/cont (accessed September 09, 2018).
[171] Chapter I, Introduction to Digital Forensics, available at: https://docplayer.net/51833294-Introduction-to-digital-forensics.html (accessed September 09, 2018).
[172] Ibid, p. 51.
[173] De Zan, T. and Autolitano, S. (2016), EUnited Against Crime: Improving Criminal Justice in European Union Cyberspace, Instituto Affari Internazionali. p.45.
[174] Ibid, p.46.
[175] Ibid, p.49.

4.1.4 Luxembourg

In Luxembourg, the rules on evidence are contained in the Code of Criminal Procedure. There are no specific admissibility conditions or restrictions for electronic evidence.[176, 177] With the Law of 18 July 2014, legislators defined seizures of "data stored, processed or transmitted in an automated data processing or transmission system".[178] Articles 31, 33 (crimes and offences in the process of being committed) and 66 (seizures ordered by an investigating judge) expressly provide for the seizure of computer data "by the seizure of either the physical device on which the data are located, or a copy".

4.1.5 The Netherlands

In the Netherlands,[179] the evidentiary system in criminal law is based on the principle of establishing the substantive truth. As expressed in the Dutch Code of Criminal Procedure a judge must be convinced by the content of the submitted legal evidence.[180] Evidence admissible under the Dutch Code of Criminal Procedure concerns the judge's own perception, statements coming from the accused, statements from a witness, statements from experts, and other relevant documents.[181] In general, the investigation, prosecution and punishment of a crime in the Netherlands are governed by the Code of Criminal Procedure, which also covers the use of special powers in case of severe crime.[182]

The relevant provisions on admissible evidence contain a few minimum rules.[183] For instance, no person should be sentenced for an offence based on assumptions established by a single statement made by one witness or by the defendant himself/herself. However, no particular provisions exist with regards to the reliability of the evidence or the proper collection of evidence. In principle, unreliable or illegally obtained evidence may be admissible in itself as legal evidence.[184] Exemptions may apply though. When the evidence is not reliable, exclusion could occur based on the principle for the pursuit of the substantive truth. On the other hand, illegally obtained evidence may be excluded after the consideration of the Court, based on a case-by-case assessment, such as the presentation of illegally gathered evidence in a court of law may be detrimental for the state, or the right of the individual to a fair trial has been infringed upon.

The Computer Crime Act III, which will enter into force in January 2019 and will be reviewed again in two years, permits law enforcement authorities to access electronic devices, including personal computers and mobile phones, in a covert and remote manner (online) as part of ongoing

[176] Council of the European Union, 7th round of Mutual Evaluations -The practical implementation and operation of European policies on prevention and combating cybercrime - Report on Luxembourg, Brussels, 2 May 2017, 7162/1/17 REV 1, p.51-52.
[177] This sub-section is based on D3.1 Regulatory Framework Analysis.
[178] Council of the European Union, 7th round of Mutual Evaluations -The practical implementation and operation of European policies on prevention and combating cybercrime - Report on Luxembourg, Brussels, 2 May 2017, 7162/1/17 REV 1, pp.51-52.
[179] Council of Europe, Status regarding Budapest Convention – The Netherlands, *coe.int*
[180] Borgers, M.J. and Stevens, L. (2010), The Use of Illegally Gathered Evidence in the Dutch Criminal Trial, Netherlands Comparative Law Association.
[181] Section 339 CCP.
[182] Odinot, G. et al. (2017), Organised Cybercrime in the Netherlands - Empirical findings and implications for law Enforcement, Dutch Ministry of Justice.
[183] Borgers, M.J. and Stevens, L. (2010), pp.18-19.
[184] Ibid, pp.1-2.

investigations and criminal proceedings, in particular in cases of serious crimes.[185] Due to the intrusive nature, the powers granted must be provided under the condition of strict oversight, including being subject to extensive judicial review, both prior to their application and during the trial stage. Proof of sufficient oversight and prior authentication may be crucial for the admissibility of the evidentiary material before a court.

4.1.6 United Kingdom

In the United Kingdom, as already mentioned in D3.1, electronic evidence is governed by the Police and Criminal Evidence Act 1984 (PACE). The two relevant clauses of PACE are Section 9(1) which allows access to excluded material or special procedure material for the purposes of a criminal investigation, and Section 19(4), which provides for acquisition of any information which is stored in electronic form and is accessible from the premises, in an legible and visible manner.[186] Examples of electronic evidence include "communications data on mobile phones, data contained in personal computers, laptops, tablets and other mobile devices, including all storage media, for example, SD cards, USB flash drives and other forms of external storage devices." Capturing and analysing data in real time using online digital forensics must be supported by appropriate legal authority.[187]

The National Police Chiefs Council defines digital forensics as "the application of science to the identification, collection, examination and analysis of electronic data whilst preserving the integrity of the information and maintaining the chain of custody of that data."[188] The Forensic Science Regulator, on the other hand, defines it as "the process by which information is extracted from data storage media (eg. devices, remote storage and systems associated with computing, imaging, image comparison, video processing and enhancement, audio analysis, satellite navigation, communications), rendered into a useable form, processed and interpreted for the purpose of obtaining intelligence for use in investigations, or evidence for use in criminal proceedings."[189]

The person in charge of the investigation has responsibility for ensuring the legality of the procedure, and the Forensic Regulator requires compliance with quality standards for digital forensics. The Association of Chief Police Officers (ACPO) has published a Good Practice Guide that provides four principles which seem to be applicable to all forms of digital evidence:

ACPO Good Practice Guide
Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.
Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

[185] Dutch government, Senate approves legislative proposal on Computer Crime III, 26 June 2018, available at: https://www.government.nl/latest/news/2018/06/26/senate-approves-legislative-proposal-on-computer-crime-iii (accessed 30 October 2018).
[186] Big Brother Watch, Police Access to Digital Evidence - The powers of the Police to examine digital devices and how forces are training staff, November 2017.
[187] Forensic Science Regulator (2014), Codes of Practice and Conduct, Appendix Digital Forensic Services, Issue 1.
[188] More info can be found here: https://www.app.college.police.uk/app-content/investigations/forensics/ (accessed September 09, 2018).
[189] Ibid.

Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Last but not least, Part 19 of the Criminal Procedure Rules describes the conditions for the drafting of the expert report and the documentation of the evidence.[190]

4.1.7 USA[191]

Since several service providers are headquartered in the USA, the relevant national legislation may be of importance here. The Federal Rules of Evidence, which were drafted in the 1960s, apply the same rules to the electronic records as they do to ordinary conventional documents; there is no specific exception for computer-generated evidence. In *Lorraine v Market American Insurance Company*,[192] the Court laid down the following broad test for admissibility of electronic records: "(i) is the information relevant; (ii)is it authentic; (iii) is it hearsay; (iv) is it original or, if it is a duplicate, is there admissible secondary evidence to support it; and (v) does its probative value survive the test of unfair prejudice?" In other words, there are three tests that an electronic record has to pass: (a) authenticity, (b) hearsay, and (c) best evidence rule. Thanks to *State v Armstead*[193] and the distinction between "computer-generated records" and "statements", many automated computer outputs are now exempt from the hearsay condition, meaning that they have to satisfy only the remaining two conditions. In USA, by not laying down any stringent conditions in the conventional evidence framework, the legislation has maintained enough flexibility for new technologies.[194]

4.2 Relevance to CYBER-TRUST

In order to explain the relevance of this section to CYBER-TRUST, we should first take a step back and briefly offer an overview of the components of the CYBER-TRUST project, as a cyber-security solution built upon three main cyber-security research pillars. These pillars, namely, are a. key proactive technologies, b. cyber-attack detection and mitigation, and c. distributed ledger technologies. A number of sophisticated methods and tools will be developed to deal with the prevention, detection, and mitigation of advanced cyberattacks involving IoT devices and networks.[195] Since the end-users of the platform may include IoT service providers, telecommunications operators, and other critical infrastructures operators, criminal investigators and Law Enforcement Agencies (LEAs and CSIRTs), and other security professionals, the legal framework presented in this document is merely the generally applicable framework with regards to evidentiary material.

[190] The Criminal Procedure Rules, Part 19 – Expert Evidence, October 2015 as amended April 2018.
[191] For a detailed analysis of the US framework on admissibility of electronic evidence, see Steven Goode, 'The Admissibility of Electronic Records' (2009) 29 Rev Litig 1.
[192] Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 (D.Md. May 4, 2007)
[193] State v. Armstead, 742 N.E.2d 720, 138 Ohio App. 3d 866.
[194] For a discussion concerning the system in India, see: Sethia, A. (2016). Rethinking admissibility of electronic evidence. International Journal of Law and Information Technology, 24(3), 229–250.
[195] CYBER-TRUST General Agreement, p.11.

Looking into the CYBER-TRUST platform, first, key proactive technologies include solutions and tools with regards to cyber-threat intelligence, cyber-threat sharing, reputation/trust management and security games. Cyber-threat intelligence refers to the information gathered before a cyber-attack is attempted. An in-depth description of cyber-threat intelligence gathering and sharing tools is found in D2.2, along with a detailed presentation of its benefits and challenges. Collected data will come from various origins, including internal, external and community sources and can range from IP and MAC addresses to news feeds or information extracted from the dark web. Some of this data may have probative value as evidentiary material.

One of those challenges, which is also critical for the legal use of the potentially evidentiary material is securing information such as controlled unclassified data and personal data and not disclosing it to unauthorised parties, which might result in infringements of the existing data protection and privacy framework. Given the applicable regulatory framework, as already explored in D3.1, the first point to consider is assess the legal ground for collecting and processing the personal data and make sure that only persons with the right authorisation are permitted to do so, for instance providing a subscription system or creating a security incident protocol, as seen in Annexes A and B.

Further concerns, with regards to cyber-threat intelligence gathering and sharing, may be minimised by the implementation of specific requirements as described in D2.2; for instance, by choosing tools which are widely accepted and approved as best practice and conform with the principles of data protection by design and by default, by deploying both human- and machine-readability to ensure that no critical information is overlooked, by designating the sensitivity or classification level of information at an early stage, by defining secure ways as to determine who is eligible to access the information, by ensuring algorithmic transparency and accountability with open-source code. Moreover, by cooperating closely with the Data Protection Officer of the organisation and conducting a Data Protection Impact Assessment, wherever regarded necessary. Organisations should undertake further measures wherever processing of special types of data takes place. Anonymisation of the information constitutes the most effective way to protect data subjects´ rights and thorough assessment, elucidating upon all crucial points in compliance with the respective legal framework, should take place before sharing the information with other authorised or competent parties. The proposed tools for this pillar of the project seem to satisfy the above standards.

As for the second pillar,[196] i.e. attack detection and mitigation, various tools that the CYBER-TRUST plans to deploy aim to the detection and mitigation of cyber-attacks against the network infrastructure, focusing on various types of DDoS attacks and identification of botnets, along with the monitoring of the network and the collection of information at real-time to provide situational awareness of ongoing incidents. The data collected from the network and registered devices will be transmitted on a fusion centre, along with intelligence gathering data, for carrying out deep learning analysis and building device profiles. Monitored indicators will be stored only if they are associated with the actionable information. To the contrary, everything that may contain evidentiary material will be maintained and will be protected with the following safeguards:

[196] Based on the CYBER-TRUST General Agreement.

- Data retention policies/ data aging;
- User and data access rights (only necessary information/data fields will be accessed by authorised users);
- Data will be digitally signed;
- Stored in an encrypted form;
- Detailed data logging system;
- Data sharing only possible through justification.

Extensions of the remote validation remediation models will be investigated in the project so as to develop efficient cyberattack mitigation strategies in decentralised IoT networks. Upon an attack, necessary files and metrics will be synched with the CYBER-TRUST backend system for further analysis while post attack observational analysis on infected files will be carried out. At the device level, proactive cyber-threat intelligence gathering has the role of identifying vulnerable files/firmware/services and notifying the device owner (passive monitoring). Additionally, CYBER-TRUST actively monitors system files and metrics for the early detection of cyber - attacks (active monitoring). Data collected depend on the defined use cases and scenarios, however, at the device level, possible personal data to be collected involve contacted IPs, destination apps and file metadata. Further data will be collected for the needs of analysis to be performed by other partners.

As extensively discussed in D3.1, pro-active cyber-threat intelligence gathering under some circumstances may amount to digital surveillance. The ECtHR[197] in *Big Brother Watch and Others v. the United Kingdom* in its judgment from 13 September 2018 expressly recognised the severity of the threats that many Contracting States currently face, including global terrorism, cybercrime and other serious crime.[198] The case looked at three different types of surveillance: the bulk interception of communications; intelligence sharing; and the obtaining of communications data from communications service providers. It acknowledged that advancements in technology have made it easier for terrorists and criminals to avoid detection on the Internet and held that States have a wide margin of appreciation in selecting and implementing the best tactics and strategies to safeguard national security. Consequently, a State may operate a bulk interception regime if it considers that it is necessary for the interests of national security. This bulk interception regime is not *per se* in violation of Article 8 of the European Convention on Human Rights.

The Court also recognised the fact that surveillance regimes have the potential to be abused, with serious consequences for individual privacy, unless they follow the six minimum safeguards defined in previous cases: the national law must clearly describe the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted must be drafted; a limit on the duration of interception must be decided; the procedure to be followed for examining, using and storing the data obtained must be established; precautions when communicating the data to other parties must be taken; and the circumstances in which intercepted data must be erased or destroyed should be determined. In the case of *Roman Zakharov v Russia*,[199] supervising the implementation of secret surveillance

[197] ECtHR, Big Brother Watch and Others v. the United Kingdom, Press release, 13 September 2018.
[198] Ibid.
[199] ECtHR [GC], judgment of 4 December 2015, Roman Zakharov v Russia, appl.no. 47143/06.

measures, alongside with notification mechanisms and remedies provided for by national law were also considered as additional effective safeguards. The Big Brother case was the first time that the Strasbourg Court considered intelligence sharing and observed that there was no evidence of any significant shortcomings in the application and operation of the surveillance regime or indeed evidence of any abuse. This is also the first case in which the Court specifically considered the extent of the interference with a person's private life that could result from the interception and examination of communications data (metadata) as opposed to content.[200]

Depending on the specific context and the purposes which the CYBER-TRUST prototype may be used for, the partners when designing the platform should take into account the above considerations, because apart from all the other implications explicitly discussed in D3.1, the manner under which data is gathered may have a serious impact on its admissibility as evidentiary material in criminal proceedings. This means that any allegedly evidentiary material, from the very first moment of its collection by the CYBER-TRUST prototype, should be treated in accordance with the principles and safeguards explained in the previous sections, as well as the national frameworks of the state where the data is going to be submitted as evidence. It is emphasised that evidence may be excluded from proceedings as a matter of law discretion, on the grounds that it is was obtained illegally, improperly or unfairly.[201] Nevertheless, the use of evidence obtained illegally under national law is not, in itself, a breach of the right to a fair trial, except for the case of entrapment.[202]

Since it becomes apparent that there is no comprehensive international or European framework, it is recommended to follow the principles introduced in the Electronic Evidence Guide and the ENISA´s Handbook on Digital Forensics concerning the proper handling of electronic evidence, which comprise the fundamental common principles found in the vast majority of national legislations: a. data integrity, ensuring that handling electronic devices and data must not cause alterations either to software or hardware. When data on a live computer system or network must be assessed, in order to avoid the loss of potential evidence, the material must be collected by an expert with the right authorisation, causing the least impact on the data; b. audit trail: all actions from the first moment of collection until the presentation of the evidentiary material before the court should be recorded in a way that if an independent third party repeats those actions in the same exact manner, it will come to the same result; c. specialist support: consultancy with experts familiar with the specific technical and legal context may be necessary; d. appropriate training: first responders must be appropriately trained to be able to search for and seize electronic evidence; e. legality: the person and agency in charge of the investigations are responsible for ensuring that the law, the general forensic and procedural principles, and all the above listed principles are adhered to with regards to the possession of and access to electronic evidence. It is of outmost importance to understand that these principles are guiding and non-binding. Therefore, the forensics expert or electronic evidence examiner must always consult with a legal expert familiar with the law of the state where the allegedly evidentiary material is taken from and the

[200] ECtHR, Big Brother Watch and Others v. the United Kingdom, Press release, 13 September 2018.
[201] ECtHR, judgment of 4 July 2002, Parris v Cyprus, appl.no. 56354/00.
[202] McBride, J. (2009), Human rights and criminal procedure - the case law of the European Court of Human Rights, Council of Europe Publishing Editions.

state where that material is going to be used for the criminal proceedings, in particular since many important European and international legal instruments are currently under reform and the legal landscape might change significantly in the near future.

During the research phase of CYBER-TRUST, only simulated data will be used, so the previous thoughts do not apply.

5. Cross-border access to electronic evidence

The cross-jurisdictional nature of cybercrime and electronic evidence poses a great challenge for the national legal frameworks, which are structured upon the notion of territoriality. Hence, quick and unhindered cooperation among law enforcement and judiciary agencies, service providers and competent authorities is crucial, not only within a state but also among diferent states.[203] In the following section, an overview of the existing and new proposed mechanisms that facilitate the exchange and transfer of electronic evidence across Europe and to third countries will be presented.

5.1 Exchange of electronic evidence across Europe

The European Union aims to create and maintain an area of freedom, security and justice, notably by facilitating judicial cooperation in criminal matters among the Member States and by fostering effective collaboration on obtaining admissible evidence.[204] To this end, the EU acknowledged the new challenges that cross-border crime, in particular cyberattacks and cybercrime entail for the administration of justice across Europe and attempted with a number of initiatives and instruments to provide mechanisms to soothe the differences in the judicial systems of the Member States and alleviate any lack of mutual recognition of judicial decisions.[205]

5.1.1 European Union

5.1.1.1 Primary law

Under Article 82(1) TFEU, judicial cooperation in the EU is based on the principle of mutual recognition of judgments and judicial decisions. According to Article 87 TFEU, police cooperation in the EU includes all competent authorities of the Member States and the EU. Based on these provisions, the EU can issue Directives and Regulations to establish and strengthen police and judicial cooperation.

5.1.1.2 Secondary law

Within the EU cooperation, mechanisms in criminal matters,[206] which facilitate cross-border investigations and coordination of prosecutions, include:[207]

- The European Investigation Order (EIO) Directive,[208] which came into force in May 2017, sets up a new system that aims to allow the EU Member States to obtain evidence from other Member States involved in criminal cases with a cross-border element, in a faster and simplified way. The EIO system aims to replace the existing EU mutual legal assistance schemes, notably the EU 2000 Convention on mutual assistance in criminal matters, and the

[203] Conclusions of the Council of the European Union on improving criminal justice in cyberspace, ST 9579/16.
[204] Communication from the Commission to the European Parliament and the Council: An area of freedom, security and justice serving the citizen, COM (2009) 262.
[205] European Commission (EC), GREEN PAPER on obtaining evidence in criminal matters from one Member State to another and securing its admissibility, Brussels, 11.11.2009, COM (2009) 624 final, p.2.
[206] European E-justice Portal - Evidence, https://e-justice.europa.eu/content_evidence-92-en.do (accessed September 10, 2018).
[207] European Commission (EC), COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD/2018/118 final - 2018/0108 (COD), Brussels, 17.04.18, p.209.
[208] 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.

European Evidence Warrant (EEW) Decision. It is essential to devote a few words to those two instruments and their relation to the EIO system. The EU 2000 Convention on mutual assistance in criminal matters entered into force in 2005, and it is still in force. Even though it did not explicitly mention neither electronic evidence nor in general, evidence for that matter, its aim was to encourage and facilitate mutual assistance between judicial, police and customs authorities on criminal matters, which might also include requests for electronic evidence, and to supplement the Council of Europe Convention on Mutual Assistance in Criminal Matters. The European Evidence Warrant system, which entered into force in 2008 and is no longer in force, was only applicable to evidence that already existed and had a minimal scope of application with respect to evidence.

The basis of the EIO Directive is the principle on mutual recognition of judicial decisions. The Directive allows the issuing authority in one Member State to request that specific criminal investigative measures be carried out by the respective executing authority in another Member State. The EIO Directive covers any investigative measure except for joint investigation teams.[209] These are covered by the Council Framework Decision 2002/465/JHA on joint investigation teams.[210] The Directive covers all types of evidence, including electronic evidence. Albeit, it does not contain any specific provisions on obtaining electronic evidence, except for Art. 10(2)(e), with reference to the identification of a person holding an IP address, for which double criminality cannot be invoked as a ground for refusal.[211]

e-CODEX is an IT system developed by the Member States to enhance cross-border judicial cooperation. It permits users, including judicial authorities, legal practitioners or citizens, to digitally exchange documents, legal forms, evidence or other information in a secure manner. e-CODEX is the cornerstone of the EIO platform.[212]

- The Council Decision 2002/187/JHA which sets up the European Union's Judicial Cooperation Unit (Eurojust)[213] and facilitates cross-border judicial cooperation in criminal matters. Moreover, the European Judicial Cybercrime Network, supported by Eurojust and

[209] European Commission (EC), COMMISSION STAFF WORKING DOCUMENT, EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT, Accompanying the document: Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD/2018/119 final - 2018/0108 (COD), Brussels, 17.4.2018.

[210] Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams.

[211] European Commission (EC), COMMISSION STAFF WORKING DOCUMENT, EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT, Accompanying the document: Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD/2018/119 final - 2018/0108 (COD), Brussels, 17.4.2018.

[212] Ibid.

[213] Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime. The Commission adopted in 2013 a proposal for a Regulation to reform Eurojust (Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust), COM/2013/0535 final. In June 2018, the two co-legislators, the European Parliament (EP) and the Council reached a political agreement on the Eurojust proposal. Its formal approval is still pending; however, the EP Plenary is scheduled to vote on the agreed text in October.

established by Council conclusions on 9 June 2016,[214] aims to foster cooperation between the competent judicial authorities dealing with cybercrime, cyber-enabled crime and investigations in cyberspace.

- The Regulation (EU) 2016/794[215] sets up the rules for the European Union Agency for Law Enforcement Cooperation (Europol), in particular, its objectives, tasks and scrutiny, including monitoring of Europol's processing of personal data.
- The Commission's Recommendation on measures to effectively tackle illegal content online from 1 March 2018,[216] which builds upon an earlier Communication from 28 September 2017,[217] indicated that removal of such content should be promoted through evidence sharing between online platforms and competent authorities.
- The Convention implementing the Schengen Agreement and its additional protocols.[218]
- The Directive 2013/40[219]: Recital 23 provides for "the cooperation between public authorities on the one hand, and the private sector and civil society on the other, is of great importance in preventing and combating attacks against information systems. It is necessary to foster and improve cooperation between service providers, producers, law enforcement bodies and judicial authorities, while fully respecting the rule of law. Such cooperation could include support by service providers in helping to preserve potential evidence, in providing elements helping to identify offenders and, as a last resort, in shutting down, completely or partially, in accordance with national law and practice, information systems or functions that have been compromised or used for illegal purposes. Member States should also consider setting up cooperation and partnership networks with service providers and producers for the exchange of information in relation to the offences within the scope of this Directive, which are further elaborated upon in Article 13."

In the next sub-sections, we will elaborate further upon the most important of those instruments.

5.1.1.2.1 The Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 2000

The Convention and its Protocol, until the entry into force of the EIO Directive, was the most commonly used instrument for obtaining evidence. It covers mutual assistance for taking statements from suspects and witnesses, the use of videoconferencing, the search and seizure to obtain evidence, telecommunications as well as information on transactions. Requesting authorities

[214] Council conclusions of 9 June 2016 on the European Judicial Cybercrime Network, 10025/16.210.
[215] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.
[216] European Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C 2018) 1177 final.
[217] European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Tackling Illegal Content Online Towards an enhanced responsibility of online platforms, COM (2017) 555 final, Brussels, 28.9.2017.
[218] The Schengen acquis - 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. 19–62.
[219] 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, p. 8–14.

may contact directly the issuing authorities. Requests should be executed the soonest possible, and by the deadline given by the requesting authority. The executing authority can refuse a request if it has grounds for such a refusal. To ensure that the obtained evidence is admissible, the authorities of the executing country must comply with the procedures specified by the authorities in the requesting country insofar as they are not contrary to fundamental principles of law in the executing country.[220]

5.1.1.2.2 The Directive on the European Investigation Order (EIO)

Since the European Evidence Warrant, the only tool that explicitly referred to electronic evidence based on the principle of mutual recognition, has failed and has been repealed, a new approach emerged that led to the creation of the European Investigation Order, with the Directive 41/2014 in April 2014.[221] Unlike the MLA, the EIO is applicable to all investigative measures aimed at obtaining evidence. The fact that the evidence already exists or not is not relevant to the EIO. It is important to note that the EIO focuses on mutual recognition of decisions made to obtain evidence.[222] Denmark and Ireland have opted out from this scheme.

According to Article 1 of the EIO Directive, a European Investigation Order (EIO) is a judicial decision which has been issued or validated by a judicial authority of a Member State ('the issuing State') to have one or several specific investigative measure(s) carried out in another Member State ('the executing State') to obtain evidence in accordance with this Directive. The EIO may also be issued for obtaining evidence that is already in possession of the competent authorities of the executing State. It covers all investigative measures except for setting up a joint investigation team, and it can be issued not only in the criminal but also in administrative or civil proceedings. The issuing authorities can only use an EIO if the investigative measure is necessary, proportionate, and allowed in similar domestic cases.[223] For the purposes of this Directive the following definitions apply: (a) 'issuing State' means the Member State in which the EIO is issued; (b) 'executing State' means the Member State executing the EIO, in which the investigative measure is to be carried out; (c) 'issuing authority' means: (i) a judge, a court, an investigating judge or a public prosecutor competent in the case concerned; or (ii) any other competent authority as defined by the issuing State with competence to order the gathering of evidence in accordance with national law; (d) 'executing authority' means an authority having competence to recognise an EIO and ensure its execution in accordance with this Directive and the national law. Such a procedure may require a court authorisation in the executing State where provided by its national law.

The Directive introduced the new principle that the executing Member State must carry out the investigative measures as swiftly as they would in similar domestic cases. The Directive also lays down the same level of priority as in national legislation and stricter time limits: maximum of 30 days to decide on recognition and execution of a request,[224] 90 days to execute investigative

[220] European E-justice Portal - Evidence, https://e-justice.europa.eu/content_evidence-92-en.do (accessed September 10, 2018).
[221] European E-justice Portal - Evidence, https://e-justice.europa.eu/content_evidence-92-en.do (accessed September 10, 2018).
[222] Rec 5 of the EIO Directive.
[223] Article 6 of the EIO Directive.
[224] Article 12(3) of the EIO Directive.

measures, following the executing decision,[225] 24 hours, where feasible, for a decision on provisional measures following the receipt of an EIO[226] and possibility for even shorter deadlines or setting specific dates. Grounds of postponement are provided for in Article 15 of the EIO Directive. The EU Member States can refuse the request on general grounds applicable to all investigative measures, namely:[227]

a. immunity or law limiting criminal liability relating to freedom of the press;
b. harm to essential national security interests;
c. non-criminal procedures;
d. *ne bis in idem* principle, in other words, no-one should be prosecuted or tried twice for the same acts, facts or behaviour;
e. extraterritoriality coupled with double criminality;
f. incompatibility with fundamental rights obligations.

Other additional grounds for refusal applicable to certain investigative measures are:

a. lack of double criminality, except for serious offences;[228]
b. impossible execution of the measure because the investigative measure is not available in similar domestic cases, and there is no alternative.[229]

According to Article 11(1) of the EIO Directive, the following measures constitute the minimum measures that must always be available under the national law:

a. the possibility to obtain information or evidence which is already in possession of the executing authority;
b. the possibility to obtain information contained in databases which the executing authority can assess directly for the purposes of the 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. all non-coercive investigative measures;
e. access to the subscriber infromation, which would enable the identification of persons who are the holders of a particular telephone number or IP address.

An executing authority shall, in accordance with its national law, guarantee the confidentiality of the facts and the substance of the EIO whereas the issuing authority shall, in accordance with its national law and unless otherwise indicated by the executing authority, not disclose any evidence or information.[230] When implementing the EIO Directive, Member States must make sure that the implementation is pursuant to the data protection framework established with the Directive (EU) 2016/680 and the principles of the Council of Europe Convention for the protection of Individuals with regard to the Automatic Processing of Personal Data of 28 January 1981 and its Additional Protocol.[231] Access to subscriber data shall be restricted, without prejudice

[225] Article 12(4) of the EIO Directive.
[226] Article 32(2) of the EIO Directive.
[227] Article 11 of the EIO Directive.
[228] Article 11(1)(g) in conjunction with Article 11(1)(h) of the EIO Directive.
[229] Article 10(5) of the EIO Directive.
[230] Article 19 of the EIO Directive.
[231] Council of Europe, *Convention for the protection of individuals with regard to automatic processing of personal data* (ETS No. 108, 28.01.1981).

to the rights of the data subject, to persons with the valid authorisation, as seen in the Deliverable D3.1. The EIO Directive was transposed in most of the EU Member States. Below is the implementation of the EIO Directive in states of relevance for CYBER-TRUST.

5.1.1.2.2.1 Cyprus

Law no. 181/2017[232] transposed the EIO Directive on 15 December 2017. As issuing and validating authority was defined the Judge of the district, who has jurisdiction to deal with the offense in respect of which an EIO was issued. As receiving authority was designated the Ministry of Justice and Public Order, which also plays the role of the central coordinating authority. Executing authorities of an EIO are a. the competent Judge with territorial jurisdiction to order such an investigative measure and b. the competent authorities which decide to take such investigative measure, i.e. the Office of the Attorney General, The Cyprus Police, The Director of Customs, The Commissioner of Taxation. Languages accepted are Greek and English.

5.1.1.2.2.2 Greece

Law no. 4489/2017, which entered into force on 21 September 2017, transposed the EIO Directive.[233] In Greece, the competent authorities to issue an EIO are: a. the judge, the court, the examining magistrate or the prosecutor and b. any other authority acting as an investigative authority in a particular criminal case. Only in the latter case, the EIO must be validated by the competent prosecutor. The Public Prosecutor at the Court of Appeal is territorially competent to recognise the EIO and ensure its execution. The same Prosecutor who receives the EIO will designate an examining judge for its execution. The Ministry of Justice, Transparency and Human Rights was designated as the central authority. Accepted languages are Greek and English.

5.1.1.2.2.3 Italy

The Legislative Decree no. 108/2017 entered into force on 28 July 2017.[234] A European Investigation Order is received and issued exclusively by the Italian Judicial Authorities, i.e. a Prosecutor of the Italian Republic or a Judge in charge of the relevant proceedings. The Authority executing an EIO shall be the Prosecutor of the Republic at the court of the main city of the district where the requested activity is requested to be carried out. If activities which need to be executed in various districts have been requested, they shall be executed by the Prosecutor of the district where most of the activities shall be performed or, if their number is the same, by the Prosecutor of the Republic of the district where the most significant investigative measure shall be carried out. When the issuing authority asks for the activity to be carried out by a judge or when the requested activity shall be carried out by a judge pursuant to Italian law, a Prosecutor of the Republic shall recognise the investigation order and ask the Pre-trial Investigation judge to execute it. The Ministry of Justice,

[232] European E-justice Portal - Evidence, https://e-justice.europa.eu/content_evidence-92-en.do (accessed September 10, 2018).
[233] European E-justice Portal - Evidence, https://e-justice.europa.eu/content_evidence-92-en.do (accessed September 10, 2018).
[234] European E-justice Portal - Evidence, https://e-justice.europa.eu/content_evidence-92-en.do (accessed September 10, 2018).

Directorate General for Criminal Justice, Ufficio II – International Cooperation was designated as the central authority. Time-wise, the requests are only accepted in Italian.

5.1.1.2.2.4 Luxembourg

The Luxembourgish Parliament has adopted the law transposing the EIO Directive on 11 July 2018. However, it has not yet entered into force.[235]

5.1.1.2.2.5 The Netherlands

The Dutch implementation law of the EIO Directive entered into force on 17 June 2017. [236] The competent authorities to issue an EIO are a. the public prosecutor, b. the examining judge and c. the court. The authority competent to receive an EIO – and also central authority - is the Centre for International Legal Assistance locally competent to execute the investigative measure, or in the cases where: a. cross border surveillance takes place, and the exact location in the Netherlands is unknown; b. the location of the investigative measure needs to be determined; the coordination of the execution of the EIO is needed because measures are required in different regions. Competent executing authorities are the public prosecutor at the local Centres for International Legal Assistance or at the National Centre for International Legal Assistance. Accepted languages are Dutch and English.

5.1.1.2.2.6 United Kingdom

The Criminal Justice (European Investigation Order) Regulations 2017 transposed the EIO Directive, entering into force on 31 July 2017 for England, Wales, Scotland and Northern Ireland and 22 May 2017 for Gibraltar.[237] Competent issuing and validating authorities are a. a designated public prosecutor; b. a judge or justice of the peace (for England); c. a judge (for Northern Ireland); a judge of the High Court or sheriff (for Scotland); The Lord Advocate or a procurator fiscal (for Scotland). Executing authorities for England, Wales and Northern Ireland are enlisted and cover different areas, such as fraud, health and general crime. Among them is The Chief Constable of the Police Service of Northern Ireland, The Chief Officer of police for a police area in England and Wales and The Director of Public Prosecutions and any Crown Prosecutor. For Scotland, the competent executing authority is the Lord Advocate. EIOs for England, Wales and Northern Ireland shall be sent to the UK Central Authority, whereas EIOs for Scotland should be sent to the Crown Office. Accepted language is English.

5.1.1.2.3 Europol and Eurojust

The European Police Office (Europol) is the EU's Law Enforcement Agency, which assists the operations and cooperation of law enforcement authorities in the EU Member States. Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU. The mandate of Europol was also under an intensive reform, which led to the

[235] Ibid.
[236] Ibid.
[237] Ibid.

adoption of the Europol Regulation in 2016.[238] The core tasks of the Agency are to collect, store, process, analyse and exchange information, including criminal intelligence, and at the same time coordinate, support and implement investigative and operational actions to strengthen the efforts of the competent national authorities.

The centrepiece of the data protection regime for Europol is the Europol Regulation, which focuses on operational personal data, i.e. personal data being processed for the objectives of the Agency. Both Europol and the Member States must implement appropriate measures, in particular with respect to automated data processing. The transfer of personal data to Union bodies, third countries, international organisations and private parties, including evidentiary material, are all covered by the principle of purpose limitation and provided for in Section 2 of the Europol Regulation. Derogations may be permitted on a case-by-case basis to safeguard a vital or legitimate interest and to prevent serious crimes.

The role of the European Union's Judicial Cooperation Unit (Eurojust), on the other hand, is to enable the cooperation between national investigative and prosecutorial authorities when working on cross-border cases. A new Eurojust regulation was also only agreed by the co-legislators in May 2018, and its adoption by the European Parliament is scheduled for October 2018.

Processing of personal data by the Union agencies in the field of law enforcement and judicial cooperation, for instance, Eurojust, is covered by the new Regulation 45/2001 through a specific chapter, which is aligned with the Directive 2016/680. Europol is excluded from this Regulation, but a review of this exclusion is scheduled for 2022.[239]

5.1.2 Why is the regulatory framework so complex and why is new legislation in EU needed?

What is most troublesome about the existing rules on obtaining evidence in criminal matters in the EU is that they are based on different co-existing levels of regulation: EU law, rules at Member State level, international conventions and bilateral agreements. The law of third countries also plays an important role, since major service providers holding relevant information that may contain evidentiary material operate under their jurisdiction. Many aspects of the relevant legal environment are currently undergoing intense reform: for instance. the e-Privacy Regulation and the e-evidence framework proposal, the drafting of the new protocol to the Council of Europe Budapest Convention concerning electronic evidence, whereas other non-EU states also engage in legislative intiatives on the matter, like the US.

The difference lays not only in the multiple applicable instruments but also in the different underlying principles, namely that of mutual assistance, in a narrower sense and that of mutual recognition, in a broader. With regard to the movement of evidence, the principle of mutual recognition means that "evidence lawfully gathered by authorities of a Member State is admissible in the courts of other Member States, taking into account the standards that apply there".[240] The

[238] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on th is based European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, *OJ L 135, 24.5.2016, p. 53–114.*

[239] European Judicial Network (EJN), New rules on data protection for EU institutions agreed, 30 May 2018, available at: https://www.ejn-crimjust.europa.eu/ejn/NewsDetail.aspx?Id=609 (accessed September 12, 2018).

[240] COM (2009) 624: Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility.

principle of mutual recognition is based on mutual trust among EU states, which presupposes that the judicial cultures share the same democratic evolution, fundamental rights guarantees and a set of standards which certify the validity and reliability of the evidence. In practice, mutual trust is a matter of judicial interpretation, meaning that admissibility and use of evidence in one Member State gathered outside of it depends upon criteria and admissibility tests established by domestic case law.[241]

This legislative patchwork makes the application of the existing framework inefficient, while it could often result in situations where other instruments, and not the most appropriate and relevant, are applied, hindering cross-border cooperation.[242] On the one hand, instruments based on the principle of mutual assistance, without any standardised form of execution, have been proven slow in several occasions, given the speed with which electronic evidence can be altered or destroyed. On the other hand, instruments based on mutual recognition, for example, the European Evidence Warrant, were also proven unsatisfactory due to their limited scope of application, meaning that they provided for a large number of grounds for refusal to execute the order.[243]

Moreover, these instruments do not only contain rules on obtaining evidence in criminal matters but also rules regarding the admissibility of evidence obtained in a different Member State than the one where the criminal proceedings take place. The reasoning behind those rules is to ensure that the evidence will not be considered inadmissible or of a minimised probative value, because of collection process followed in another Member State. Nevertheless, these rules are far from creating a common standard, making it quite likely that admissibility chances are higher for states with similar national criminal justice systems and lower for states which follow different approaches.

With electronic evidence being stored increasingly on private infrastructures and with inefficiencies in public and private cooperations between service providers[244] and public authorities, as well as shortcomings in defining jurisdiction, effective investigations and prosecutions seem to be hampered.[245] A final concern is about the fact that information that is currently publicly available and accessible by Law Enforcement Agencies may in the near future be stored into systems requiring special access rights, for instance, the domain names platform "WHOIS".

All in all, the fragmentation in legislation as well as in case law results in legal uncertainty and has a negative impact on the protection of fundamental rights. Improving cross-border access

[241] Ibid.

[242] European Commission (EC), GREEN PAPER on obtaining evidence in criminal matters from one Member State to another and securing its admissibility, Brussels, 11.11.2009, COM (2009) 624 final, p.4.

[243] Ibid.

[244]Ibid. "The Yahoo! and Skype decisions in Belgium are examples of recent court cases which focus on the legitimacy of the use of domestic production orders for companies whose main seat is outside the requesting country but which provide a service in the territory of that country. In addition, there have been a number of court cases in the US on whether US authorities have the right to request the production of data stored abroad by a service provider whose main seat is in the US, including notably the "Microsoft Ireland" case."

[245] European Commission (EC), COMMISSION STAFF WORKING DOCUMENT, EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT, Accompanying the document: Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD/2018/119 final - 2018/0108 (COD), Brussels, 17.4.2018.

to electronic evidence becomes imperative,[246] and thus, new legislation is currently being negotiated.

5.1.3 New proposed electronic evidence framework

Given all the aforementioned concerns, the European Commission proposed on 17 April 2018 new rules in the form of two Regulations and a Directive. With the new European Production Order, judicial authorities in one Member State will be allowed to obtain electronic evidence directly from a service provider or its legal representative in another Member State within 10 days in regular cases, and within 6 hours in case of emergency.[247] [248] Moreover, with the new European Preservation Order, judicial authorities in one Member State will be permitted to request that a service provider or its legal representative in another Member State preserves specific data in view of a subsequent request to produce this data. The proposed package also includes a draft Directive which would provide minimum rules for the appointment of a legal representative for service providers not established in the EU.

The proposal strengthens the individuals´ rights, by ensuring access to legal remedies and clarifies the prevalence of the General Data Protection Regulation and the Directive 2016/680, as transposed in the Member State law. Only stored data is covered by the orders since the real-time interception of telecommunications is not covered by this proposal. Two obligations are established for the authorities in the proposal: a. to receive approval for all the orders from a judicial authority, and b. to ensure that their legality, necessity and proportionality have been checked. Production orders to produce transactional or content data may only be issued for serious criminal offences, specific cybercrimes and terrorism-related crimes, as defined in the context of the proposal. On the other hand, productions orders for subscriber data or access data can be produced for all criminal offences. The European Data Protection Board recalls that electronic evidence may include all these four categories of data and that regardless of whether this data is categorised as content or non-content data, all these categories are to be considered personal data, since it may be related to an identified or identifiable natural person.[249]

Concerning the new obligations of the service providers, the proposed legislation might be of high relevance to the CYBER-TRUST project with regards to the end-users of the prototype. Specifically, both the European Preservation Order and the European Production Order are legally binding and will make it mandatory for service providers to produce electronic evidence. The proposal seems to actually be based on the principle that cooperation should take place between an authority and a service provider rather than between two authorities.[250] The legislative proposal expands the scope of application and includes obligations for providers of services that are used for

[246] Ibid.
[247] Ibid.
[248] Currently the time can be up to 120 days for the existing European Investigation Order or an average of 10 months for a Mutual Legal Assistance procedure.
[249] European Data Protection Board, Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b), adopted on 26 September 2018, p.11.
[250] Ibid, p.4.

communication purposes,[251] providers of information society services that enable interactions between users and that are used for the storage of data,[252] and providers of internet infrastructure services[253] when all of them are offering services in the European Union, irrespective of the place of the data storage (disappearance of the location criteria).[254]

5.2 Transfer of electronic evidence to/from third countries

The transfers of electronic evidence to and from third countries (other than the EU Member States) are based on international law, and more specifically on multilateral and bilateral agreements. At the Council of Europe level, the 2011 Convention on Cybercrime (Budapest Convention) provides a framework for mutual legal assistance and a first definition of electronic evidence. The Parties to the Convention are currently negotiating an additional protocol dealing with cross-border access to electronic evidence. Furthermore, the European Convention on Mutual Assistance in Criminal Matters of the Council of Europe of 20 April 1959 and its additional protocols, alongside with bilateral agreements concluded under Article 26 are still used by the states in the context of police and judicial cooperation.[255] [256]

Between the EU and the EU Member States, on the one hand, and other third countries, on the other, there is an abundance of bilateral agreements, such as the 2000 Agreement on Mutual Legal Assistance between the EU and the US. The EU-US Umbrella Agreement complements existing EU-US and Member State – US agreements with a comprehensive data protection framework enhancing EU-US law enforcement cooperation. The EU-US Privacy Shield, a data-sharing agreement which ensures the flow of personal information for commercial purposes across the Atlantic, is also relevant.

5.2.1 The CoE Cybercrime Convention

Chapter three of the Cybercrime Convention regulates international cooperation with regards both to the prosecution of cybercrime and the collection of evidence in electronic form. The three general principles concerning international cooperation thus include extensive cooperation related to all evidence exchange and transfer, cooperation with regard to all criminal offences related to computer systems and data, and cooperation in accordance with the Convention and other relevant international agreements pertaining to criminal matters.[257] The cooperation scheme provided by the Convention is grounded on the principles of extradition and mutual assistance. From those two, we will look into mutual assistance.

[251] Including providers of telecommunications services and other electronic communications services, including interpersonal communications services.
[252] Including online marketplaces that facilitate peer-to-peer transactions and providers of cloud computing services.
[253] Including registries that assign domain names and IP addresses important for the functioning of the internet.
[254] The requested data must be (1) needed for a criminal proceeding for which the issuing authority is competent and (2) related to services of a provider offering services in the Union. If this is the case, the data must be preserved and produced.
[255] Council of Europe, European Convention on Mutual Assistance in Criminal Matters, ETS no.030, Strasbourg, 20/04/1959.
[256] European E-justice Portal - Evidence, https://e-justice.europa.eu/content_evidence-92-en.do (accessed September 10, 2018).
[257] Council of Europe, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, CETS 185, para 254.

5.2.1.1 Mutual Assistance

Chapter Three, section One, title 3 of the Cybercrime Convention provides the general principles relating to mutual assistance. Article 25 provides the general principles relating to mutual assistance. With a mutual assistance request, the requesting state may obtain electronic evidence gathered abroad for use in domestic criminal proceedings. To ensure admissibility, the collection of the evidence will have to meet the requirements set by the requested state. State Parties to the Convention shall grant one another mutual assistance to the widest extent possible. Nevertheless, intrusive measures can only be requested, under the condition that proper safeguards for the rights and the freedoms of individuals affected by such an intrusion are in place in the requested state.[258]

The availability of cooperation mechanisms and investigative measures, in particular those described in articles 29 – 35 of the Convention, is vital for effective cooperation in computer related criminal offences. These mechanisms include (many of them were discussed in Section 3.2.2):

- Spontaneous information (Art. 26);
- Procedures related to mutual assistance requests in the absence of applicable international agreements (Art. 27);
- Confidentiality and limitation on use (Art. 28);
- Expedited preservation of stored computer data (Art. 29);
- Expedited disclosure of preserved traffic data (Art. 30);
- Mutual assistance regarding accessing stored computer data (Art. 31);
- Cross-border access to stored computer data upon consent or where publicly available (Art. 32);
- Mutual assistance in the real-time collection of traffic data (Art. 33);
- Mutual assistance regarding the interception of content data (Art. 34);
- 24/7 Network (Art. 35).

Mutual assistance is a formal process, which has been proven lengthy and bureaucratical and thus, it is often complemented by informal police-to-police or agency-to-agency (prior) communication. In such informal communication, the assistance of international Law Enforcement Agencies such as Interpol or Europol may prove useful. Furthermore, Article 25(3) provides for an accelerated process through urgent requests and the set of shorter deadlines. Article 25 (5) provides that the condition of dual criminality shall be deemed present if the conduct for which assistance is sought is also a criminal offence under the requested State Party's laws, even if its laws classify the offence within a different category or use divergent terminology.[259]

5.2.2 New proposed framework

In parallel with the EU legislative procedure described in Section 5.1.3, the Parties to the Budapest Convention have been currently discussing the creation of a second protocol concerning the "Enhanced international cooperation on cybercrime and electronic evidence" explicitly addressing the aforementioned matters regarding electronic evidence.[260] Even though the negotiations are not

[258] Council of Europe, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, CETS 185, para 257.
[259] Council of Europe, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, CETS 185.
[260] Council of Europe, Enhanced international cooperation on cybercrime and electronic evidence: Towards a Protocol to the Budapest Convention, 19 March 2018.

to be concluded before 2019, the main issues to be addressed are the following:[261] a. the need to differentiate between subscriber, traffic and content data in terms of requirements and thresholds for access to data needed in specific criminal investigations; b. the limited effectiveness of mutual legal assistance for securing electronic evidence; c. situations of loss of location of data and the fact that States increasingly resort to unilateral trans-border access to data in the absence of international rules; d. the question as to when a service provider is sufficiently present or offering a service in the territory of a Party; e. the current regime of voluntary disclosure of data by US-providers; f. the question of expedited disclosure to data in emergency situations; g. data protection and other safeguards. The potential adoption of this Protocol in conjunction with the new proposed EU framework, is of high significance for the CYBER-TRUST project, as it might affect its use and objectives in the future.

5.3 At the national level

Some EU Member States, except for bilateral agreements with other states within or outside the EU, have adopted provisions in their domestic legislation to forward cross-border access to electronic evidence through direct access.[262] In Italy for instance, given the increasing number of requests, the Ministry of Justice issued a memorandum in 2015 that allows Italian judges to directly ask for assistance from their foreign peers, skipping the step that required political approval for sending a request.[263] The memorandum also maintains that direct contact between judicial authorities should be preferred, as opposed to involving the Ministry of Justice, which instead should be dealing with MLATs requiring the Ministry and diplomatic approval.

Since many service providers whose cooperation is required to obtain certain types of electronic evidence have their main establishment in the US or other non-EU countries, the domestic frameworks of those non-EU states is also of relevance in this context.[264]

5.4 Relevance to CYBER-TRUST

Since cybercrime does not know borders, the possibility of exchange and transfer of evidentiary material seems quite likely in the CYBER-TRUST context, after the launch of the prototype. In that case, depending again on the end-users, the main instruments shaping the current legal framework for cross-border access to evidence, as seen above, consists of bilateral and multi-lateral mutual legal assistance (MLA) agreements replaced as of 22 May 2017 within the EU by the European Investigation Order (EIO) but still used in some contexts, the Budapest Convention, and national laws and procedures of Member States and third countries.

[261] Smuha, N.A., Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency in: EuCLR European Criminal Law Review, pp. 83 – 115.
[262] Council of Europe, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, CETS 185.
[263] European Commission (2016), Questionnaire on improving criminal justice in cyberspace - Summary of Responses.
[264] European Commission (EC), COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD/2018/118 final - 2018/0108 (COD), Brussels, 17.04.18.

Cross-border access to electronic evidence may be acquired:[265]

- Through the means of formal cooperation between the relevant authorities of two states, usually via an MLA or an EIO in EU, or informal police-to-police cooperation;
- through direct contact with law enforcement authorities of one state and service providers whose main establishment is in another state, either on a voluntary or mandatory basis; for example, service providers established in the United States cooperate on a voluntary basis, as far as the requests concern non-content data;[266]
- through direct access, pursuant to the national legislation.

[265] Non-paper from the Commission services, Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward, June 2017, p.1.
[266] European Commission (2016), Questionnaire on improving criminal justice in cyberspace - Summary of Responses.

6. The legal dimensions of the use of DLT systems for the storage of evidentiary material

In this section, we will discuss the legal implications of the use of Distributed Ledger Technologies (DLT) in the context of law enforcement and specifically, for the storage of electronic information that may contain evidentiary material. In order to do that, we will first provide the reader with the crucial definitions, we will distinguish between Blockchain and DLT systems, and then we will dive into the data protection framework and other relevant legal issues.

6.1 Definitions

Up until now, there seems to be no universal and coherent definition for what is referred to as a DLT system. On top of that, there is no common terminology for its components either. The existing definitions are either too technical and inaccessible to a general audience or too broad and simplistic, resulting in misconceptions and confusion.[267] Even though there is no common definition, which is also partially due to the lack of ad-hoc regulation as well as to the fact that the technology is still in its infancy, many attempts in literature are worthwhile to be presented, in order to understand better the idea behind the use of DLT for the storage of information which may contain evidentiary material in the CYBER-TRUST context. The World Bank (2017) describes DLT systems as "a specific implementation of the broader category of 'shared ledgers', which are simply defined as a shared record of data across different parties".[268] Tasca and Tessone (2018) define a DLT system as "a community consensus-based distributed ledger where the storage of data is not based on chains of blocks".[269]

As in the case of electronic and digital evidence above, the terms "Distributed Ledger Technology" and "Blockchain" are often used interchangeably. Distributed Ledger Technology is an umbrella term as the underlying technology, whereas Blockchain was the first fully functional system, hence, a DLT subcategory. Cong & He (2018) defines a blockchain as a "distributed database that autonomously maintains a continuously growing list of public records in unit of 'blocks', secured from tampering and revision", while Atzori (2015) describes it as an "irreversible and tamper-proof public records repository for documents, contracts, properties, and assets [that] can be used to embed information and instructions, with a wide range of applications".[270] Other definitions classify blockchain technology based on the dimension of authority and the incentive to participate, the principles of archival science, or its data diffusion models and on-chain functionality.[271]

In this document, we will use the term "Distributed Ledger Technologies", because it is wide enough to cover the technical choices in CYBER-TRUST and we will follow the latest definition and general approach proposed by Rauchs et al.,[272] that focuses on the essential minimum requirements of a DLT system, based on an extensive literature review on the topic. Given that DLT systems are a

[267] Rauchs, M. et al. (2018), Distributed Ledger Technology Systems, A conceptual framework, University of Cambridge.
[268] Ibid.
[269] Tasca, P. and Tessone, C. (2018), Taxonomy of Blockchain Technologies. Principles of Identification and Classification, available at: SSRN: https://ssrn.com/abstract=2977811 (accessed 30 October 2018), p.3.
[270] Rauchs, M. et al. (2018).
[271] UK Government Office for Science (2016), Distributed Ledger Technology – Beyond Blockchain, A report by the UK Government Chief Scientific Adviser.
[272] Rauchs, M. et al. (2018).

type of distributed systems, which exhibit a set of specific characteristics that distinguish them from more traditional distributed systems, Rauchs et al. (2018) define a DLT as "a system of electronic records that enables a network of independent participants to establish a consensus around the authoritative ordering of cryptographically-validated ('signed') transactions. These records are made persistent by replicating the data across multiple nodes, and tamper-evident by linking them by cryptographic hashes. The shared result of the reconciliation/consensus process - the 'ledger' - serves as the authoritative version for these records."[273] A "ledger", in turn, is created, maintained and updated collectively by multiple parties, which can validate the transactions independently and ensure the system integrity.[274]

6.2 Features of the DLT system

6.2.1 Actors

Actors can determine the operation and governance of a DLT system and shape its properties. As actors are identified legal entities or natural persons who have different roles in the system[275]. Sometimes, they can play multiple roles and operate in more than one layers. Actors can be grouped into four main categories:[276] developers, administrators, getaways and participants. The relations among all those actors are governed by a system of checks and balances so that no single party can control the system unilaterally.[277] The *developers* are in charge of composing and maintaining the underlying code. *Administrators* have the control of the codebase repository and decide when to alter the system rules. *Getaways* provide the interfaces to the system, while *participants* can be entrusted with a wide range of tasks. For example, *fully-validating nodes or auditors* check the validity of submitted records; *miners or validators* produce sets of records that could be potentially included in the ledger; *end-users* have specific actions assigned to them.

6.2.2 Layers

Although there are many different categorisations in the literature concerning the layers of DLT systems, for reasons of consistency we will also follow here the approach of Rauchs et al. DLT systems consist of three layers that are interdependent, meaning that the higher level cannot exist without the lower one.[278] Seen in a pyramidic scheme, their order reflects conceptual and functional dependencies. First at the bottom of the pyramid lays the protocol level; second, in the middle, comes the network level; and third, the data level on the top. The protocol and network layers enable the construction and maintenance of the data layer: a shared database created by a multi-party consensus. The network can impact the data layer, whereas the protocol layer can impact both the network and the data layer. It follows that whoever has control over the protocol layer can influence both the network and the data layer.

[273] Rauchs, M. et al. (2018).
[274] Ibid.
[275] Ibid, p.29-30.
[276] Ibid.
[277] Ibid.
[278] Ibid.

The *protocol layer* includes the software that is implemented by the network layer, which "defines, manages and updates the global ruleset that governs the system".[279] In this layer,[280] its components will determine whether the system is self-sufficient or whether it is dependent on another system; moreover, in this layer the developers will create a codebase or re-purpose an existing one, to serve as the foundation of the DLT system; lastly the ruleset that will govern the DLT system will be decided. The protocol layer also defines the decision-making process which is required for the alteration of the protocol itself in a legitimate manner and the implementation of changes to the protocol rules.

The *network layer* consists of a system of independent servers and storage that collectively participate in the operations defined by the protocol rules.[281] The network involves several participants who do not necessarily know or trust one another but who contribute to the network in exchange for rewards. In the network layer it is specified which actors can have access to the network (*open v closed*), how data is shared (*public v private*) and who has the authorisation to initiate transactions (*unrestricted v restricted*) as well as who of the participants can update the shared set of records (*permissionless v permissioned*), how participants will reach an agreement for the implementation of these updates and how they can verify actions and records.

The *data layer* refers to the processing and storage of information, which take the form or records.[282] The DLT system creates a shared data structure – the ledger, as seen above. The data layer governs how and which data is used in the creation and addition of new records, including smart contracts and the content of the blocks.

6.2.3 Consensus algorithms

A transaction will be added to the set of authoritative records only once its validity is verified. For a transaction to be validated, it has to be correctly formatted in line with the protocol rules and to not contain any conflicting elements. Records are subject to the consensus algorithm, a process which determines their validity or invalidity and selects among equally valid records, without the need to rely on a central authority.[283] As seen above, depending on the design choice, producing new candidate records can be permitted to any network participant (*permissionless*) or only to a specific subset of participants (*permissioned*). There are different consensus algorithms, that have been developed from the early days of DLT systems up until today, including Proof-of-Work, Proof-of-Stake, Proof-of-Authority, Proof of Elapsed Time, Byzantine Fault Tolerance, Proof-of-Activity, Proof-of-Importance, Proof-of-Capacity, Proof-of-Burn, Proof-of-Weight.[284]

For instance, Bitcoin introduced the Proof-of-Work consensus algorithm.[285] In the Proof-of-Work scheme – a more centralised solution - miners, using significant computational power, solve

[279] Hill, R., Boffins: Confusing distributed ledger tech definitions create 'unrealistic expectations' about what it can do - Report proposes tight conceptual DLT framework,14 August 2018, *Theregister.co.uk*
[280] The description and distinction of the layers, as well as the whole Section 6.2 is based on the very comprehensive analysis of Rauchs, M. et al. (2018), p.34.
[281] Ibid, p.35.
[282] Ibid, p.36.
[283] KPMG, Consensus Immutable agreement for the Internet of value, June 2016, p.1.
[284] Anwar, H., Consensus Algorithms: The Root Of The Blockchain Technology, 25 August 2018, *101blockchains.com*
[285] Ibid.

highly complex mathematical puzzles, in order for a new block to be created and confirmed and they receive back one coin for each newly added block. In the Proof-of-Stake (e.g. Ethereum) – a more decentralised solution - individuals who can mine or validate new blocks are pre-selected, based on their coin pre-possession and they get to receive a proportional reward which mirrors their mining contribution and their initial possession of coins.[286] In Proof-of-Authority, a small group of formally identified validators is pre-approved to validate transactions and blocks, and low computational power is required.[287]

6.2.4 Understanding centralisation v decentralisation

When speaking about a DLT system, decentralisation is always brought up as one of its core advantages. A decentralised option must provide for processes which allow free and open participation to all. In that case, the decision-making is not adhered to a fixed fraction of entities or individuals. Since a DLT system is created by various processes and subsystems, different degrees of decentralisation can be detected at each layer or even within the same layer.[288] Hierarchal schemes can assist with determining the potential source of authority but dynamics in a DLT system can be rather fluid, which further complicates a definitive assessment of the system as "centralised" or "decentralised". DLT systems such as Bitcoin, in other words open, public, and permissionless, opt for full decentralisation, for instance, within the aim to achieve censorship resistance and improve system resilience.

Decentralised Autonomous Organisations (DAO),[289] a new type of smart-contract-based decentralised communities, have been organised alongside the decentralised model. As these new organisations are based on the DLT and therefore do not adhere to a specified jurisdiction, the applicable law and national legal status for such DAOs are yet to be determined.

6.2.5 Design choices

Notwithstanding to centralisation and decentralisation options, different needs and objectives require suitable design choices. Every system relies upon these costs and benefits trade-offs to achieve its objectives and build security, trust, and threat models.[290] Design configurations at one layer of a DLT system can impact other layers or components and lead to different system characteristics. For instance, the presence of trust in a system (e.g. banks which use a closed DLT system) allows for a more flexible design approach than a DLT system which is based on minimum trust conditions. Furthermore, DLT systems which put particular emphasis on keeping all aspects of their system "decentralised", may improve censorship resistance but they will possibly have to deal,

[286] Ibid.
[287] Curran, B. What is Proof of Authority Consensus? Staking Your Identity on The Blockchain, 5 July 2018, *Blockonomi.com*
[288] Rauchs, M. et al. (2018), pp.29-30.
[289] Blemus, S. (2017), Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide, Corporate Finance and Capital Markets Law Review, RTDF N°4-2017, December 2017
[290] Ibid, p.43.

on the other hand, with inefficient redundancy, slow verification speed, poor user experience and high energy consumption costs.[291]

Nevertheless, every design choice comes at the expense of other system properties or an increase in the system's centralisation. Decisions upon choosing a more centralised or decentralised design, for instance, could come at the expense of the complexity and the size of the ledger, minimising its desired functions.[292] Similarly, choosing one consensus mechanism over another may affect the security of the system.[293] Furthermore, even though there is a widespread belief that records stored on a DLT system are "immutable", DLT systems provide different degrees of transaction finality, meaning that an executed transaction may be subject to reversal under specific circumstances and design choices.[294]

Consequently, any design choice will also trigger different legal considerations, given the characteristics that each system takes, in combination with its different uses and applications. As discussed further in Section 6.4.2, choosing one or another design could make compliance with GDPR and in general data protection frameworks easier or impossible.[295] Threats to the systems include not only attacks by external entities, but also actions by internal stakeholders and failure of core components, such as software.[296] Prior to any implementation, detailed threat models need to be developed, and specific security requirements should be identified, to deliver the outcome of what design fits better the needs of the CYBER-TRUST platform.

6.3 Implications with the European legal framework

6.3.1 Lack of *ad hoc* regulation

The use of DLTs, being an innovative technology that can have such a broad variety of potential use cases, still under rapid development and intense experimentation, requires legal and regulatory clarification which is rather challenging.[297] In the European Union, despite its well-developed legal environment, there are fundamental areas that this technology touches upon, in which there is little or no regulatory clarity or conformity. Some Member States are more ahead than others, which choose to fill these gaps with case law and judicial interpretation, given the specific application and use (e.g. financial sector and cryptocurrency). However, the judicial process can be slow, and yet the rulings in one country are not binding on the rulings of another. Moreover, many areas remain under national competence. Nonetheless, regarding the use of DLTs for law enforcement purposes, there is little, if not at all legal guidance.[298]

[291] Hill, R., Boffins: Confusing distributed ledger tech definitions create 'unrealistic expectations' about what it can do - Report proposes tight conceptual DLT framework, 14 August 2018, *Theregister.co.uk*
[292] Rauchs, M. et al. (2018), p.46.
[293] Ibid.
[294] Ibid.
[295] Commission Nationale de l'Informatique et des Libertés (CNIL), Blockchain et RGPD: quelles solutions pour un usage responsable en présence de données personnelles ?, 24September 2018.
[296] UK Government Office for Science (2016), Distributed Ledger Technology – Beyond Blockchain, A report by the UK Government Chief Scientific Adviser.
[297] The European Union Blockchain Observatory and Forum, Thematic Report, Blockchain Innovation in Europe, 21 August 2018, p.16.
[298] Finck, M. (2017), Blockchains: Regulating the unknown, German Law Journal Vol. 19 No. 04.

6.3.2 GDPR considerations

However, that does not entail that GDPR "exist[s] in a regulatory vacuum".[299] To the contrary, it is only one part of a constellation of many EU or Member State instruments which regulate a plethora of fields which DLT applications are related to or can have an impact upon. One of those legal instruments is the General Data Protection Regulation. Reconciling the GDPR with DLT may prove challenging. The GDPR has a dual objective: on the one hand, to protect the rights of individuals and on the other, facilitate the free flow of personal data within the EU. Moreover, the right to the protection of personal data is not an absolute right, as discussed in D3.1 and must be balanced against other fundamental rights, in line with the principle of proportionality.[300]

The GDPR applies to personal data, regardless of the technology used. However, the law was drafted before DLT systems became widely used. Having a centralised system in mind for collecting, storing and processing data, the legislator did not take into consideration the decentralised features of a DLT. In D3.1, we initially discussed whether the activity of collecting, storing and processing data in DLT falls within the scope of the EU's data protection regime or not. It is important to understand that GDPR compliance (or compliance with Directive 2016/680 in the law enforcement context) can only be assessed with regard to use cases and applications and not to the DLT as a new technology.[301] In this deliverable, we will dive further into defining whether or how GDPR as a legal instrument which mostly addresses centralised solutions, can apply to a decentralised system.

6.3.2.1 Personal data

Article 4 GDPR – Definitions
For the purposes of this Regulation:

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

As discussed in D3,1, depending on the respective DLTs´ use cases, data stored in blocks may be data related to an identified or identifiable individual, such as data related to behaviour in a network of connected devices. This data could be stored in three formats: a. in plain text, b. in encrypted form, or c. as hashes to the chain.[302] Data stored on a ledger in plain text is clearly still personal data under GDPR and encrypted data as well, since it can still be accessed with the correct keys. Personal data which has been processed through a hashing function may also continue to qualify as personal data under GDPR.[303] However, further clarification is needed in the case when the actual personal

[299] The European Union Blockchain Observatory and Forum, Thematic Report, Blockchain and the GDPR, 16 October 2018.
[300] Ibid, p.24.
[301] The European Union Blockchain Observatory and Forum, Thematic Report, Blockchain and the GDPR, 16 October 2018, p. 4.
[302] Finck, M. (2018), Blockchains and Data Protection in the European Union, European Data Protection Law Review, 4 (1), pp. 17 – 35.
[303] Ibid.

data is kept off-chain, and this off-chain data is later erased so that the hashed data should once again be considered anonymous.[304]

The discussion around a user's public key is slightly more complicated. As seen in D3.1, a public key is data that "can no longer be attributed to a specific data subject", however, if matched with "additional information" such as a name or an address, it could result in the identification of a user.[305] Unlike the aforementioned data, public keys cannot be moved off-chain, since they are essential components of the DLT system. Nevertheless, public keys will most likely not be considered personal data in the following circumstances: a. when the public key does not belong to a natural person; or is not created on behalf of a natural person; or does not point to personal data; or when the key cannot be associated to a data subject by any reasonable means and is therefore truly anonymous.[306]

When the public keys fall under the scope of the GDPR, it is more challenging to identify GDPR-compliant solutions. Moreover, concerning the technical and organisational measures by default concerning purpose and storage limitation, given that every full node has at its disposal a complete copy of each blockchain and that a new block is added to the complete preceding chain, this provision cannot be complied with in respect of public keys. The only way to ensure compliance would be to recognise specific GDPR compliant key-handling techniques.[307]

Some solutions constitute the use of a stealth addresses or of state channels for two-side smart contracts that only share information with outside parties in the event of a dispute, or the addition of "noise" to the data.[308] From all those techniques, the Article 29 Data Protection Working Party has admitted that the addition of noise may be an acceptable anonymisation technique in combination with "the removal of obvious attributes and quasi-identifiers".[309,310] Nevertheless, there have been incidents, where the partial leakage of non-personal information allowed the application of statistical attacks to de-anonymise repeated transactions, through the so-called Statistical Disclosure Attacks, whose effectiveness yet is an open question.[311]

When considering the use of encryption, obfuscation and aggregation techniques in the CYBER-TRUST context, the partners must take into consideration all these issues before choosing the type of DLT system and its particular characteristics, as well as the inclusion of personal data in a DLT system or not. First of all, the storage of personal data on-chain should, if possible, be avoided. Second, the partners should make sure before choosing cryptographic techniques, that they have assessed any possible reversal risks – whether the cryptographic process could be reversed and the data be reconstructed, for instance by using brute force decryption – and any potential linkability

[304] The European Union Blockchain Observatory and Forum, Thematic Report, Blockchain and the GDPR, 16 October 2018, p.21.
[305] Ibid.
[306] Blockchain Bundesverband, Blockchain, Data Protection and the GDPR, 25 May 2018, *bundesblock.de*
[307] Ibid.
[308] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014, 0829/14/EN WP216, p.12.
[309] Ibid.
[310] Ibid.
[311] UK Government Office for Science (2016), Distributed Ledger Technology – Beyond Blockchain, A report by the UK Government Chief Scientific Adviser, p.51.

risks – whether encrypted data can still be linked to an individual by examining contextual patterns or with the use of additional information.[312]

6.3.2.2 Data controllers and processors

Article 4 GDPR – Definitions
For the purposes of this Regulation:
(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Art. 26 GDPR - Joint controllers
Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.

Where there is processing of personal data in DLT systems, accountability can be a convoluted issue. One aspect of accountability is the identification of the data controllers and subsequently processors. For instance, in private DLTs, it might be possible to identify a central system operator as the data controller who will receive the subjects´ requests and claims. In public DLTs, though, there is no central point of control as the network is operated by all nodes in a decentralised mode. This way, it appears that the Regulation's obligations would rest on each node independently, meaning that data subjects can invoke claims from each node.[313] Determining that each node is a data controller raises significant complications, since the exact number, location and identity of nodes on a chain may be rather challenging to be established.

According to the French Data Protection Authority, the participants of a blockchain, for instance, should be considered data controllers, when they have the right to write on the blockchain and submit data for validation.[314] Participants, irrespective of being natural persons or legal entities, could be considered data controllers if they process the personal data in relation to a professional or commercial activity and they write the personal data on the blockchain. Consequently, miners who do not intervene in the transactions or other persons who do not process the data for commercial or professional purposes are not to be considered data controllers (given the household exception of Article 2 GDPR).[315]

In the case of more participants with the same rights (for instance in the case of a group of organisations working towards a common cause), by default, the French Data Protection Authority argues that they should all be considered as joint data controllers and they should determine their responsibilities and roles in a transparent manner in order to comply with the provisions of GDPR.

[312] The European Union Blockchain Observatory and Forum, Thematic Report, Blockchain and the GDPR, 16 October 2018.
[313] Finck, M. (2018): "Nodes do not, in principle, qualify as 'joint controllers' under Article 26(1) GDPR as they do not 'jointly determine the purposes and means of processing'."
[314] Commission Nationale de l'Informatique et des Libertés (CNIL), Premiers éléments d'analyse de la CNIL – Blockchain, September 2018, p.2.
[315] Ibid, p.3.

Alternatively, they could designate one of them as data controller or create a legal entity, which would be considered as data controller.[316] Under specific circumstances, the miners who process personal data and the developers of a protocol or smart contract, who process personal data on behalf of a participant – data controller, may qualify as data processors. In that case, they should comply with the obligations of data processors as laid out in Article 28 GDPR.[317]

6.3.2.3 Jurisdiction and territoriality

Permissionless DLTs, moreover, usually run on nodes located in various jurisdictions across the globe raise jurisdictional questions pertaining to the application of European data protection requirements to the transfer of data to third countries.[318] The GDPR provides that a "transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation" shall only occur subject to a number of specific conditions, as seen in D3.1.[319] Compliance with this provision in a permissionless DLT would be almost impossible, since the data stored in blocks are hashed to the chain by randomly selected miners that can be based anywhere in the world, even in states or organisations which do not offer an adequate level of data protection. Nevertheless, compliance with GDPR standards could also be problematic for permissioned DLT systems, which have a global scope of operation even though the identity of the data controllers and processors might be known, since the latter may not be able to guarantee the necessary additional safeguards or may be established in states which do not provide the necessary adequacy level.[320]

6.3.2.4 Enforcement of data subject´s rights

Under the Regulation, data subjects hold certain rights, as discussed in detail in D3.1. First, the use of DLTs, depending on the design choice, seems to have an impact on the obligation for data minimisation and respectively to the right to rectification, when the data is not accurate (article 16 of the GDPR) and the right to erasure (article 17 of the GDPR), when the data cannot be easily erased. The immutability of the data written on the ledger could pose challenges for the effective enforcement of those two rights, if the code cannot be amended and data written on it are kept, in principle, forever.[321] It is argued though that nodes can be changed[322] either by court order or by the miners themselves, depending on the type of the DLT and its governance scheme. If that was an actual possibility, it could raise another issue. If nodes as verification means were to be modified or deleted, the integrity of the DLT, as a secure storage solution for electronic evidence might be compromised.

According to the French Data Protection Authority, it seems technically impossible to comply with these two rights, as long as personal data is stored on the blockchain, either in plain text or

[316] Ibid, p.4.
[317] Ibid, p.5.
[318] Finck, M. (2018).
[319] Article 44 of the GDPR.
[320] The European Union Blockchain Observatory and Forum, Thematic Report, Blockchain and the GDPR, 16 October 2018, p.26.
[321] Jensen, G. Reconciling GDPR rights to Erasure and Rectification of Personal Data with Blockchain, *oracle.com*
[322] Accenture has patented a scheme for editing a permissioned blockchain which leaves a "scar".

hashed. Thus, it is strongly recommended to not store any personal data on the blockchain and instead to use a cryptographic method to encrypt the data. If a request for erasure is received by the data controller, then deleting the secret key of the hashing function, could have an effect similar to erasure, but it does not constitute erasure *stricto sensu*.[323] Nevertheless, it is underlined that "erasure" is not defined in the GDPR, letting other interpretations than absolute deletion to emerge.[324] As for the right to rectification of incorrect data, it is important to keep in mind that a later transaction can always cancel an earlier transaction. The data controller can add the correct data on a new block and initiate a new transaction, which would cancel the earlier one. Even though the earlier transaction containing the erroneous data will always be registered in the blockchain, it is possible to use similar techniques like in the case of erasure, if the inaccurate data must be deleted.[325]

Similar questions arise from the right of the data subject to access the information, either by confirming that their data is being processed and for what purposes or request a copy of it. Except for the difficulty of identifying a data controller, which might be overcome in a permissioned DLT, data controllers most likely will not know which data is stored on-chain as they often only handle the encrypted or hashed version thereof.[326] The French Data Protection Authority, on the other hand, recognises that the right to information and access, as well as the right to data portability, can be compatible with the technical features of a blockchain and do not raise particular concerns.[327]

Another issue emerges regarding the Data Privacy Impact Assessment (DPIA). The controller must carry out a DPIA when the processing is "likely to result in a high risk to the rights and freedoms of natural persons".[328] A DPIA is mandatory for large-scale processing activities, and a DLT could fall within this category as long as personal data is stored on-chain. Nevertheless, it is not clear as to how a controller can determine the scope of the DPIA on a DLT system and, in the case of vague definition of roles, under which conditions the DPIA should be conducted.

Last but not least, the right to restriction of processing and the prohibition of being subject to automated decision-making may be compatible in the context of a blockchain, but they are also further discussed in the context of smart contracts in Section 6.3.2.6.

6.3.2.5 Data protection by Design and by Default

Art. 25 GDPR Data protection by design and by default

1. *Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed*

[323] Commission Nationale de l'Informatique et des Libertés (CNIL), Premiers éléments d'analyse de la CNIL – Blockchain, September 2018.
[324] Finck, M. (2018), p. 25.
[325] Commission Nationale de l'Informatique et des Libertés (CNIL), Premiers éléments d'analyse de la CNIL – Blockchain, September 2018, p.9.
[326] Jensen, G. Reconciling GDPR rights to Erasure and Rectification of Personal Data with Blockchain, *oracle.com*.
[327] Commission Nationale de l'Informatique et des Libertés (CNIL), Premiers éléments d'analyse de la CNIL – Blockchain, September 2018.
[328] Article 35 of the GDPR.

to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. *The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. [3]In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*

Data protection by design and data protection by default are two overarching guiding principles of the GDPR. According to them, data controllers shall, both during the design of the processing operation and at the time of the processing itself, implement appropriate technical and organisational measures. Systems architects must, from the beginning, account for the GDPR's objectives, considering data minimisation, storage limitation and pseudonymisation or anonymisation techniques as well as data security measures, for instance when choosing the consensus model. Minimising on-chain data could be achieved by moving it, as far as possible, off-chain.[329]

6.3.2.6 Smart contracts

"Programmatically-executed transactions (PETs) are computer scripts that, when triggered by a particular message, are executed by the system".[330] When the code operates as intended, the level of trust among the contracting parties can be minimum.[331] Even though smart contracts are a technology *per se*, there is still no unanimous definition, mainly because the term "contract" can receive a different meaning depending on whether it is perceived by a computer scientist or a legal expert. Legal scholars define a contract as a legally binding agreement between two or more parties, whereas computer engineers conceive it as computer code. This distinction has sparked a vivid debate as to whether code can be law. In the EU, the concept of "smart contract" has been scrutinized in an in-depth analysis by the European Parliamentary Research Service in 2017[332], but no political will is present for the adoption of an EU regulation any time soon.[333] Without a clear definition and an unambiguous legal status, "smart contracts" may still be subject to the application of existing legislation, for instance, contract law as defined in the respective jurisdiction.[334]

Nick Szabo offered a detailed description of "smart contract" back in 1994: "a computerized transaction protocol that executes terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions, minimize exceptions both malicious and

[329] Recital 28 GDPR.
[330] Rauchs, M. et al. (2018).
[331] Ibid.
[332] See: European Parliament, How blockchain technology could change our lives, In-depth analysis, February 2017, PE581.948.
[333] European Parliament, Distributed Ledger Technology And Financial Markets, Briefing, November 2016. See also the recent European Parliament Resolution of 3 October 2018 on distributed ledger technologies and blockchains: building trust with disintermediation (2017/2772(RSP)).
[334] Cooper, B., The Current State Of Blockchain Regulation, 30 May 2017, *mobilepaymentstoday.com*.

accidental, and reduce the need for trusted intermediaries."[335] More recently, the UK government chief scientific adviser proposed another definition: "contracts whose terms are recorded in a computer language. These contracts can be automatically executed by a computing system, such as a suitable distributed-ledger system. Potential benefits include low contracting, enforcement, and compliance costs, while potential risks include reliance on the computing system that executes the contract".[336]

According to the French Data Protection Authority, the creator of the algorithm of the smart contract may be simply a facilitator of a technical solution.[337] However, depending on his/her involvement in the determination of the processing purposes, he/she could be considered a data processor or controller.[338] The criteria for identifying a data controller or a data processor in the smart contract context are not easy to be defined, in particular, because once deployed, the smart contract is executed independently from its publisher.[339]

Moreover, Article 22 GDPR gives data subjects the right to be protected from automated processing of information. It is still unclear how this provision could affect the operation of smart contracts, in particular when a data subject has the right to request human intervention and ask for explanations with regards to how a decision was made.[340] Automated decision-making is in the core of a smart contract and is necessary for its execution, as far as it allows for the fulfilment of the contract obligations. The data controller must assure that the concerned persons have access to human intervention, the possibility to have their opinion heard and and the right to file a complaint against the decision that was taken, even after the execution of the smart contract.[341] For that to happen, the possibility for human intervention must be guaranteed, irrespectively from what is written in the blockchain.

As for the right to restriction of processing, restrictions can be included in smart contracts, as long as such a restriction is added to the code, before the execution of the transaction.[342] At the moment, a case-by-case assessment seems to be the solution.[343]

6.3.2.7 Off-chain v On-chain considerations

The term "off-chain" refers to anything that happens outside of the boundaries of a DLT system. This is opposite to the "on-chain" which refers to anything that occurs within the DLT system. A GDPR-compliant solution for the use of DLTs for the storage of evidentiary material is the storage of information including personal data off-chain and the storage of the reference to this data on-

[335] Szabo, N. (1994), Smart contracts, available at: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (accessed 30 October 2018).
[336] European Parliament, Distributed Ledger Technology And Financial Markets, Briefing, November 2016.
[337] Commission Nationale de l'Informatique et des Libertés (CNIL), Premiers éléments d'analyse de la CNIL – Blockchain, September 2018.
[338] Ibid.
[339] Ibid.
[340] The European Union Blockchain Observatory and Forum, Thematic Report, Blockchain and the GDPR, 16 October 2018, p.18.
[341] Ibid.
[342] Ibid.
[343] Ibid.

chain.[344] Emphasis should be put on the fact that this off-chain database is under the scope of GDPR or the Directive 2016/680, depending on the circumstances, and should be in compliance with all the relevant provisions governing databases. Moreover, concerning the on-chain data, see Section 6.3.2.1.

6.3.2.8 Data security

6.3.2.8.1 Private keys

Users communicate their transactions by adding a cryptographic signature for authentication purposes. Nevertheless, a valid signature does not guarantee that it is the owner of the corresponding private key who has produced the signature. Instead, it only guarantees that the holder of a private key at a specific time has initiated a transaction.[345] Thus, it is important to note that private keys can be stolen by attackers if they are not properly secured, raising serious data security concerns.[346] Storing private keys in a secure manner would be optimal. However, such a solution requires a high level of technical expertise, which is why this task is usually outsourced to third parties.

6.3.2.8.2 Censorship resistance and 51% attacks

Censorship resistance is a term commonly used in the context of DLT which generally refers to the inability of a single party or group to unilaterally change the rules of the system, block or censor transactions. A so-called 51% attack against a DLT system occurs when an entity or group with a majority of the "votes" (for example, computing power) produces records faster than the rest of the network, taking control over the system.[347] In some cases and under specific circumstances, DLT systems may be affected by attacks carried out by less than 51% of voting power, again putting at stake the data security and system integrity.[348]

6.3.3 Chain of custody

One of the main challenges as seen above is the proper management of material that may contain electronic evidence, from the very first moment this information is acquired till its presentation in the court of law, in other words, the chain of custody or evidence. The latter plays an important role that may affect whether the evidence will be finally admitted or not in the legal proceedings. However, the chain of custody should be always followed by forensic and legal experts in all circumstances, due to the sensitive character of the information it may contain.[349]

In criminal proceedings, DLTs could be used to track the chain of custody when evidence is captured, gathered and taken later for analysis. Storing evidence in the DLT would include the generation of a digital fingerprint, known as "hash", which is unique to each digital asset. The potential use of a DLT system for the chain of custody was explained in D3.1, Section 7.3.3. If a proper solution with regards to personal data is adopted, the storage of evidence in DLT seems to

[344] McKinlay et al., Blockchain: Challenges And Legal Issues Of New Technology, 2 February 2018, *dlapiper.com*
[345] Rauchs et al. (2018), p.28.
[346] Zyskind, G. et al (2015), Decentralizing Privacy: Using Blockchain to Protect Personal Data, *2015 IEEE Security and Privacy Workshops*, San Jose, CA, pp. 180-184.
[347] Rauchs, M. et al. (2018), p.62.
[348] Ibid.
[349] Bonomi, S. et al., B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics, available at: https://arxiv.org/pdf/1807.10359.pdf

satisfy to some extent all the conditions described both in ENISA´s and CoE´s guides on electronic evidence, specifically, the traceability, the verifiability, the security and data integrity, and the audit trail.[350] A DLT-based chain of custody architecture, built upon a private and permissioned DLT or a similar solution would be favourable, for this way unauthorised and untrusted parties would be prevented from joining the network and excluded from having access to it.

However, admissibility of the evidence before the Court will still have to be discussed on a case-by-case basis and in accordance with the relevant national law and case law of the Member State, where the criminal proceedings take place.

6.4 Relevance to CYBER-TRUST

The CYBER-TRUST project aims to utilise DLT´s capabilities and structures of enabling a comprehensive view of transactions back to origination in order to store safely material that may contain electronic evidence. There seems to be a tendency worldwide in the police and security sector to centralise the collection of evidence and case files. However, a centralised system has to be secure enough so that its very structure does not leave it vulnerable to exploitation.[351] This is where DLTs could contribute, ensuring that no single party can control the system, reducing this way the risk of manipulation and the danger of information being tampered with. Nevertheless, the practice is far from common, and there is no case law to draw conclusions from yet.

The idea behind a DLT system is to decentralise the control over the data, by using powerful encryption to create hashes or digital signatures of a dataset and share the data widely across a network of different computers, where anyone who has access to the system can check and verify the validity of the records. Each of those hashes or digital signatures is attached to others to form an unbreakable in a cryptographic sense chain, forming block additions and executing transactions.[352] In the chain of evidence, instead of transactions, the blockchain is envisaged to record all the subsequent steps in the evidential process, from the moment of the first collection of the alleged electronic evidence. Nevertheless, it is only the encrypted digital signature recorded in the ledger; the details of the investigation must remain secure and confidential. When the evidentiary material is passed to the court, the full history of the evidence file can be verified independently.[353]

The CYBER-TRUST project relies on a concept, which includes the following phases:

- Registration. When an IoT product is assembled, it is registered into a DLT marking the beginning of its life;
- Update. Upon change, e.g. update of the product's firmware, a new fingerprint is generated and submitted to the network of peers;

[350] ENISA, Electronic evidence - a basic guide for First Responders Good practice material for CERT first responders [2014], p. 5 –8. These principles are discussed in more detail in the handbook: ENISA, Identification and handling of electronic evidence –Handbook, document for teachers [2013] September 2013. The principles used by ENISA are the same principles used by the Council of Europe in its Electronic Evidence Guide.
[351] Open Trading Network, UK Police — Blockchain solutions on the horizon, 3 December 2017, *medium.com*
[352] Blockchain and Digital Chain of Evidence, 13 March 2018, *Kinesense-vca.com*
[353] Ibid.

- Verification. At any point in time, the network peers can quickly verify the properties of an IoT device by regenerating the cryptographic fingerprint.

Concerning modelling, deciding whether the permissioned or permissionless solution will be used, where the former can either be public or private and the choice of the consensus protocol, it is evident that different objectives require different design choices. Design configurations at one layer of a DLT system can impact other layers or components and lead to different system characteristics, imposing a trade-off of costs and benefits, as seen in Section 6.2.5. For any choice, given the legal *lacunae* in the field, guiding force should be the enforcement of data subject´s rights and data security, as long as personal data is being processed.

Although techniques used at the moment for storing personal data on-chain do not seem to be out of the scope of GDPR, this might not always be the case in the near future.[354] Both of the following ideas are of relevance for CYBER-TRUST. First, since the use of DLT systems becomes more and more common, there will be soon cases where courts or the European Data Protection Board will be called to decide upon whether some cryptographic processes can be considered capable of anonymisation or at least, offer protection equal to anonymisation.[355] Moreover, the European Data Protection Supervisor has already announced the creation of guidelines on the matter until the end of 2018, whereas the French Data Protection Authority (CNIL) and the European Union Blockchain Observatory and Forum have already published their first reports on Blockchain and data protection.[356] Such judgments and guidelines can create more certainty from a legal and technical point of view, enabling developers to choose the correct cryptographic tools for their applications, while encouraging them to create tools based on specifications, legally recognised as anonymisation techniques and in general, as appropriate organisational and technological measures.

Second, technical solutions are currently being developed in order to achieve GDPR compliance, that may result that transactional data will not be directly stored in the blockchain.[357] For instance, personal data could be stored off-chain and linked to the blockchain through a hash pointer. Extra safeguards would need to be put in place in that case, in order to secure the stability and availability of the off-chain database. Only encrypted, hashed personal data would be stored on the DLT system and if a data erasure request is received, deletion of the encryption key(s) could make the data unrecoverable, the closest to full erasure than can be done up till present.[358] The encryption key(s) should not be stored on the blockchain as the blockchain would not allow their deletion. Instead, they should be themselves encrypted with the use of a “master” encryption key.[359]

Another concept is that of Zero Knowledge Proofs, which allow someone who has in his/her possession data to show that they actually have it without revealing the content of the data.[360] Furthermore, homomorphic encryption techniques are advanced cryptographic methods that allow

[354] Ibid.
[355] Ibid.
[356] Commission Nationale de l'Informatique et des Libertés (CNIL), Premiers éléments d’analyse de la CNIL – Blockchain, September 2018.
[357] Finck, M. (2018).
[358] Jensen, G. Reconciling GDPR rights to Erasure and Rectification of Personal Data with Blockchain, *oracle.com*
[359] Ibid.
[360] Blockchain Bundesverband, Blockchain, Data Protection and the GDPR, 25 May 2018, *bundesblock.de*

distributed computations to be performed by private servers.[361] Data aggregation techniques on the top of obfuscation and encryption techniques can be another secure solution, for example, by aggregating large amounts of data from many data subjects into a single digital signature that is added to the ledger, as a proof-of-existence of the original data. It is to be noted that the Article 29 Working Party admits that there are inherent limitations in most anonymisation and pseudonymisation techniques.[362] Thus, when selecting and implementing the techniques or a combination of them, all means reasonably likely to be used to identify an individual must be taken into consideration, both internally and by other third entities/individuals, especially when additional data sets could be obtained and used to lead to the identification of an individual. Keeping up with technological developments in the field of encryption and re-assessing regularly the effectiveness of anonymisation or pseudonymisation techniques may also lead to higher protection levels.

Metadata should also be treated appropriately as it could reveal personal information even where personal data is not directly stored on-chain. Organisational and technical measures, as well as emergency plans, must be put in place to prevent or mitigate 51% attacks and limit the impact of algorithmic fallacies, in particular, those related to encryption.[363] Furthermore, organisational and technical measures must be implemented for the management of the different permissions, as well as for the documentation of changes in the governance or the software used for the execution of the transactions.[364]

If the aforementioned features are guaranteed and if the collection of evidence has followed the legal requirements and principles described both in ENISA´s and CoE´s guides on electronic evidence and the national framework of the jurisdiction where the evidence is going to be used for the criminal proceedings, then the evidentiary material would have a good chance to be admissible. A DLT-based chain of custody architecture built on a private and permissioned blockchain or a similar solution would be favourable.

[361] The European Union Blockchain Observatory and Forum, Thematic Report, Blockchain and the GDPR, 16 October 2018, p.23.
[362] Commission Nationale de l'Informatique et des Libertés (CNIL), Premiers éléments d'analyse de la CNIL – Blockchain, September 2018
[363] Ibid, p.11.
[364] Ibid.

7. Conclusions

7.1 Overview of the implications for CYBER-TRUST

7.1.1 Admissibility of evidentiary material

Given the applicable regulatory framework as already explored in D3.1, the first thing to consider is assess the legal ground for collecting and processing any personal data and make sure that only persons with the right authorisation are permitted to have access. Depending on the specific context and the purpose which the CYBER-TRUST prototype may be used for, the partners when designing the system should take into account the above considerations, because apart from all the other implications explicitly discussed in D3.1, the manner under which data is gathered, handled and preserved may have a serious impact on its admissibility as evidentiary material in criminal proceedings. This means that any allegedly evidentiary material, from the very first moment of its collection by the CYBER-TRUST prototype, should be treated in accordance with the principles and safeguards explained in the previous sections, as well as the national frameworks of the state where the data is going to be submitted as evidence. It is emphasised that evidence may be excluded from proceedings as a matter of law discretion, on the grounds that it was obtained illegally, improperly or unfairly.[365]

Since there is no comprehensive international or European framework, it is recommended to follow the principles introduced in the Electronic Evidence Guide and the ENISA´s Handbook on Digital Forensics concerning the proper handling of electronic evidence, which comprise the fundamental common principles found in the vast majority of national legislations: a. data integrity: ensuring that handling electronic devices and data must not cause alterations either to software or hardware. When data on a live computer system or network must be assessed, in order to avoid the loss of potential evidence, the material must be collected by an expert with the right authorisation, causing the least impact on the data; b. audit trail: all actions from the first moment of collection until the presentation of the evidentiary material before the court should be recorded in a way that if an independent third party repeats those actions in the same exact manner, it will come to the same result; c. specialist support: consultancy with external experts familiar with the specific technical and legal context may be necessary; d. appropriate training: first responders must be appropriately trained to be able to search for and seize electronic evidence; e. legality: the person and agency in charge of the investigations are responsible for ensuring that the law, the general forensic and procedural principles, and all the above listed principles are adhered to with regards to the possession of and access to electronic evidence. It is of outmost importance to understand that these principles are guiding and non-binding. Therefore, the forensics expert or electronic evidence examiner must always consult with a legal expert familiar with the law of the state where the allegedly evidentiary material is gathered from and the state where that material is going to be used for the criminal proceedings. During the research phase, only simulated data will be used, so the previous thoughts do not apply.

[365] ECtHR, Parris v Cyprus (dec.), 56354/00, 4 July 2002. See also: The Modern Law of Evidence, Adrian Keane, Oxford University Press, 2008, page 53.

7.1.2 Cross-border access to electronic evidence

Since cybercrime does not know borders, the possibility of exchange and transfer of evidentiary material seems quite likely in the CYBER-TRUST context, both between public authorities but also between public authorities and service providers. In that case, depending again on the end-users of the prototype, electronic evidence may be obtained through formal cooperation channels between the relevant authorities of two countries, usually through a MLA or an EIO in EU, or police-to-police cooperation; through direct cooperation between law enforcement authorities of one country and service providers whose main establishment is in another country, either on a voluntary or mandatory basis; through direct access, if allowed by Member State's national legislation.

However, the European Commission proposed in April 2018 new rules in the form of two Regulations and a Directive, aiming to create a European Production Order, which will allow a judicial authority in one Member State to obtain electronic evidence directly from a service provider or its legal representative in another Member State within 10 days in regular cases, and within 6 hours in cases of emergency; and a European Preservation Order, which will allow a judicial authority in one Member State to request that a service provider or its legal representative in another Member State preserves specific data in view of a subsequent request to produce this data. The Council of Europe also works on the creation of an additional Protocol expressly related to cross-border access to electronic evidence.

7.1.3 Use of DLT systems for the storage of evidentiary material

The CYBER-TRUST project aims to utilise DLT´s capabilities and structures to store material that may contain electronic evidence. Although there seems to be a tendency worldwide in the police and security sector to centralise the collection of evidence and case files, the idea behind a DLT system is to decentralise the control over the data.[366] In the chain of evidence, instead of transactions, the DLT system is envisaged to record all the subsequent steps in the evidential process. Nevertheless, it is only the encrypted digital signature recorded in the ledger. When the evidentiary material is passed to the court, the full history of the evidence file can be verified independently.[367]

Deciding whether the permissioned or permissionless model will be used, where the former can either be public or private and choosing the consensus protocol, it is evident that different objectives require different design choices, which will lead to different system characteristics, imposing a trade-off of costs and benefits. For any choice, given the legal *lacunae* in the field, guiding force should be the enforcement of data subject´s rights, data security and data minimisation, as long as personal data is being processed.

Although techniques used at the moment for storing personal data on-chain do not seem to be out of the scope of GDPR, this might not always be the case in the near future.[368] First, guidelines from stakeholders and judgments from national and European courts can create more certainty from a legal and technical point of view, leading to the creation of proper tools. Second, technical solutions are currently being developed in order to achieve GDPR compliance, that may result that

[366] Blockchain and Digital Chain of Evidence, 13 March 2018, *Kinesense-vca.com*
[367] Ibid.
[368] Ibid.

personal data will not be directly stored in the ledger. Data aggregation techniques on the top of obfuscation and encryption techniques can be another secure solution. It is to be noted, though, that the Article 29 Working Party admits that there are inherent limitations in most anonymisation and pseudonymisation techniques.[369] Thus, when selecting and implementing the techniques or a combination of them, all means reasonably likely to be used to identify an individual must be taken into consideration, both internally and by other third entities/individuals, especially when additional data sets could be obtained and used to lead to the identification of an individual.

Third, keeping up with technological developments in the field of encryption and re-assessing regularly the effectiveness of anonymisation or pseudonymisation techniques may also lead to higher protection levels. Organisational and technical measures, as well as emergency plans must be put in place to prevent or mitigate 51% attacks and limit the impact of algorithmic fallacies and to ensure efficient management of the different permissions, as well as documentation of changes in the governance or the software used for the execution of the transactions.[370]

If the aforementioned features are guaranteed and if the collection of evidence has followed the legal requirements and principles described both in ENISA´s and CoE´s guides on electronic evidence and the national framework of the jurisdiction where the evidence is going to be used for the criminal proceedings, then the evidentiary material would have a good chance to be admissible. A DLT-based chain of custody structured upon a private and permissioned blockchain or a similar solution would be favourable. Albeit, admissibility of evidentiary material will have to be discussed on a case-by-case base and in accordance with the relevant national law and case law of the Member State, where the criminal proceedings take place, always under the guidance of a legal expert familiar with the local legal framework and forensics specialists for each specific type of evidence.

7.2 Final remarks

Section 1 presented the purpose and outline of the document, as well as the scope and intended audience. Section 2 shed light on the definition of electronic evidence, as opposed to conventional evidence, the particular features of electronic evidence and digital evidence, the sources and types of electronic evidence. A sub-section was devoted to the status quo of digital forensics and the current best practice. Section 3 gave an overview of the international and European framework concerning electronic evidence, while Section 4 focused on the national framework in selected Member States of relevance for CYBER-TRUST (Cyprus, Greece, Italy, Luxembourg, The Netherlands and the United Kingdom as well as the USA), with emphasis to the admissibility of electronic evidence, the investigative powers and the digital forensics. Section 5 gave insight to the complex legal system that governs the cross-border access to electronic evidence. Section 6 introduced the legal implications of the use of DLT systems for the storage of electronic evidence. Section 7 concluded with an overview of the implications for CYBER-TRUST and final remarks.

[369] Ibid.
[370] Ibid.

Annex A – Case study: investigation of a DDoS attack in Greece

Here follows a case study, based on the insights of the Hellenic Police, which participates in the CYBER-TRUST consortium through KEMEA, as the beneficiary entity in Security Research projects, in accordance with the *Memorandum of Cooperation* (MoC) signed between Hellenic Police and KEMEA.[371]

For this case study, the investigated cyber-attack is presumably a Distributed Denial of Services, and the involved actors are a. the affected telecommunications provider, b. the police officers in charge of the crime investigation, c. the prosecutor and other relevant competent authorities in Greece who ordered the investigation, d. the respective prosecutor and other relevant competent authorities in an EU Member State or in a third country and e. the suspect(s) located in Greece or elsewhere. The process undertaken by the Hellenic Police is described in five steps and depends on whether the alleged crime is characterised by a cross-border element.

(Step 1) According to Article 4 Section 8 of the Law 3649/2008, the National Intelligence Service (National Computer Emergency Response Team) is the agency which is concerned with the prevention and mitigation of cyber-attacks against public entities and National Critical Infrastructure. Based on Article 292B of the Greek Criminal Code (GCC) the criminal proceedings for this specific type of offence depending on the severity of the attacks may be initiated either when the victim of the alleged crime files a complaint or on the Prosecutor`s own motion. The latter may be the case, for instance, if the attack caused a denial of service that lasted for a very long period of time or a vital infrastructure was affected. Given their significance for the protection of the functions of the society, telecommunication networks may be considered vital, in particular as long as they constitute part of infrastructure that provides the population with goods or services of vital importance. The Prosecutor may be notified by the National Intelligence Service, the affected telecommunications provider, or any other public authority or individual aware of the incident (Articles 37, 40 and 42 of the Greek Criminal Code) and will call for the proper investigation of the allegations.

(Step 2) Police officers of the Cybercrime Division of the Hellenic Police, with the right authorisation, will access the premises of the telecommunications provider in order to secure the crime scene, identify and collect the necessary electronic evidence and take depositions from the concerned employees. The collection of evidentiary material may consist of three different approaches based on the incident and the equipment targeted by the cyber-attack:

i. Seizure of the Terminal/Server/Hard disk(s), cataloguing the hardware that was seized and transfering it to the Forensic Science Division of the Hellenic Police for further examination;
ii. On the fly imaging of the hard disks;
iii. Live forensics. In this latter case, police officers from the Forensic Science Division will also, in principle, be present at the premises of the Telecommunication provider besides the officers of the Cybercrime Division.

(Step 3) The next step is the forensic analysis of the collected evidentiary material by the police officers of the Forensic Science Division. The analysis is based on specific criteria and

[371] Grant Agreement, p.56.

questions provided by the Cybercrime Division. These criteria and questions differ based on each occasion.

(Step 4) When the forensic analysis is finished, the findings are then transferred from the Forensic Science Division to the Cybercrime Division to be included in the case file.

(Step 5) Assuming that the investigators discovered the IP address(es) allegedly responsible for the DDoS attack, the Cyber-crime Division will search if the IP address(es) are located in Greece or not:

i. In case the IP address is located in Greece and given the severity of the alleged crime, the prosecutor may give a formal warrant to the police to proceed with all the necessary investigative measures, for instance the search of the suspect´s residence, arrest of the suspect or/and seizure of all relevant electronic devices that may contain evidentiary material, which will be identified, collected, preserved and analysed as described in Steps 2, 3 and 4. Based on the findings, charges may be filed against the individual(s), and the criminal proceedings may continue, in accordance with the Greek Criminal Procedure Code.

ii. In case the IP address is not located in Greece, then it will either be located:

a. within the EU; or
b. outside the EU.

In case (a), if the IP address is located in one of EU Member States, which are members of Europol (European Law Enforcement Organisation), the Hellenic Police will submit a request to Europol to coordinate with the national police of the country where the IP address is located.

In case (b), if the IP address is not located in an EU Member State, then the Hellenic Police will submit a request to Interpol[372] to coordinate with the national police of the country where the IP address is located.

It is of note that this procedure of establishing a first contact with Europol and Interpol, and via them with the Law Enforcement Agencies of the concerned countries, aims to the exchange of information within the framework of informal police cooperation in order to initially assess the case and to determine whether to proceed or not with a Mutual Legal Assistance request, which is lengthier and more formal. The latter is made by the competent judicial authorities of the requesting state (i.e. Greece) by issuing and submitting an International Letter of Request (ILOR) based on Article 457 of the Greek Criminal Code to the competent authority of the country where the IP address is located.

(Step 6) In both cases, depending on the measures requested by the Greek authority, the competent authorities of the receiving state are obliged to respond to the request as soon as possible and comply with the requested investigative measures. These measures may include the processes described under Step 2 and will be performed in accordance with the national legislation both of the requesting and the receiving state, in order for the collected evidence to be admissible before the Greek Court. Once the receiving state responds that the competent authorities have

[372] Interpol is the world's largest international police organization, with 192 Member States as of 2018.

gathered the requested material, the Greek competent authorities may request its transfer, and once the evidentiary material is received, it will be added to the case file.

If the circumstances are such, the Greek State may request the extradition of the suspect in order to be brought before its courts and judged under national law. The country that receives the extradition request can either accept or decline based on various grounds, for instance, the lack of double criminality. If the case is brought before a Greek Court, the procedural law does not include rules concerning the probative value of the various means of evidence, and therefore, all lawfully acquired evidence may be admissible, as discussed in Section 4.1.2.

Annex B - Case study: Telecommunications service provider incident management procedure

The incident management procedure of a telecommunication service provider when an alleged security incident occurs may include the following four steps. In the first step, namely the detection and reporting of the incident, employees, contractors or third parties become aware of or detect an alleged security incident and report it via the appropriate channel to the persons in charge of the IT infrastructure. They will proceed with an initial diagnosis of the situation or will contact the competent Information Security Officer, which will then proceed with the diagnosis herself. Either way, the IT infrastructure department or the Information Security Officer will attempt to figure out whether it is a known or an unknown threat. If it is a known threat, the second step is skipped, and the third step is triggered. If it is an unknown threat, then the incident is reported to the relevant stakeholders and the second step is initiated.

The second step is the incident analysis and includes the incident prioritisation, the collection of potentially evidentiary material and the performance of root-cause analysis. Once the incident analysis is complete, the third step deals with the incident resolution and communication. The persons in charge of the procedure are entrusted with the task of resolving the incident, preparing an incident report, notifying all relevant stakeholders and taking preventive and further corrective actions.

The fourth and final step is the root incident analysis. The persons in charge perform post-incident analysis and create user awareness. Last, the Information Security Officer concludes the procedure by updating the known problems database.

8. References

8.1 Literature

Biasiotti, et al. (2018), Handling and Exchanging Electronic Evidence Across Europe, Springer International Publishing.

Blemus, S. (2017), Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide, Corporate Finance and Capital Markets Law Review, RTDF N°4-2017, December 2017.

Borgers, M.J. and Stevens, L. (2010), The Use of Illegally Gathered Evidence in the Dutch Criminal Trial, Netherlands Comparative Law Association.

Borgers, M.J. and Stevens, L. (2010), The Use of Illegally Gathered Evidence in the Dutch Criminal Trial, Netherlands Comparative Law Association.

Brown CSD (2015) Investigating and Prosecuting Cyber Crime: Forensics Dependencies and Barriers to Justice, International Journal of Cyber Criminology 9, pp. 55–119.

Casey, E. (2000), Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet with Cdrom (1st ed.). Academic Press, Inc., Orlando, USA.

Casey, E. (2011), Digital Evidence in the Courtroom, in Digital Evidence and Computer Crime, Third Edition, pp.49-83.

Casey, E. (2011), Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press, Inc., Orlando, FL, USA.

De Zan, T. and Autolitano, S. (2016), EUnited Against Crime: Improving Criminal Justice in European Union Cyberspace, Instituto Affari Internazionali.

Divakaran, D.M., et al. (2017), Evidence gathering for network security and forensics, Digital Investigation Vol.20, Supplement (March 2017), pp. S56-S65.

Finck, M. (2017), Blockchains: Regulating the unknown, German Law Journal Vol. 19 No. 04.

Finck, M. (2018), Blockchains and Data Protection in the European Union, European Data Protection Law Review, 4 (1), pp. 17 – 35.

Forgó, N., et al. (2018), Privacy Protection in Exchanging Electronic Evidence in Europe, in: Handling and Exchanging Electronic Evidence Across Europe, pp. 255–288.

Hamidovic, H. et al. (2016), The basic steps of digital evidence handling process, International Journal of information and communication technologies, Vol. 2.

Insa, F., The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime-Results of a European Study, in Journal of Digital Forensic Practice, 2006.

Keane, A. (2008), The Modern Law of Evidence, Oxford University Press.

Mason, S. (2007), Electronic Evidence - Discovery & Admissibility, LexisNexis Butterworths, London.

Mason, S. (2008), International Electronic Evidence, British Institute of International and Comparative Law.

McBride, J. (2009), Human rights and criminal procedure - the case law of the European Court of Human Rights, Council of Europe Publishing Editions.

Mitja, G., et al. (eds.) (2014), The Italian Code of Criminal Procedure. Critical Essays and English Translation, CEDAM and Wolters Kluwer Italia.

Mohay, G. M. et al. (2003), Computer and Intrusion Forensics, Artech House, USA.

Odinot, G. et al. (2017), Organised Cybercrime in the Netherlands - Empirical findings and implications for law Enforcement, Dutch Ministry of Justice.

Palmer, A. (2018), Mutual Legal Assistance: Understanding the Challenges for Law Enforcement in Global Cybercrime Cases, Center for Cyber and Homeland Security, The George Washington University, Issue Brief – January 2018.

Quinn, P. (2016), D2.1 Report on the Data Protection, Privacy, Ethical and Criminal Law Framework Deliverable, FORENSOR project.

Rauchs, M. et al. (2018), Distributed Ledger Technology Systems, A conceptual framework, University of Cambridge.

Sethia, A. (2016), Rethinking admissibility of electronic evidence. International Journal of Law and Information Technology, 24(3), pp. 229–250.

Smuha, N.A., Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency in EuCLR European Criminal Law Review, pp. 83 – 115.
Steven Goode, 'The Admissibility of Electronic Records' (2009) 29 Rev Litig 1.
Summers, S. (2007), Fair Trials - The European Criminal Procedural Tradition and the European Court of Human Rights, Hart Publishing.
Tasca, P. and Tessone, C. (2018), Taxonomy of Blockchain Technologies. Principles of Identification and Classification, available at: SSRN: https://ssrn.com/abstract=2977811 (accessed 30 October 2018).
Vatis, M. A. (2010), The Council of Europe Convention on Cybercrime, in: Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.
Vuille, J. et al. (2017), Scientific evidence and the right to a fair trial under Article 6 ECHR, Law, Probability and Risk, Volume 16, Issue 1, 1 March 2017, pp. 55–68.
Zyskind, G. et al. (2015), Decentralizing Privacy: Using Blockchain to Protect Personal Data, 2015 IEEE Security and Privacy Workshops, San Jose, CA, pp. 180-184.

8.2 Case law

European Court of Human Rights (Council of Europe)

ECtHR, judgment of 19 February 1991, Isgrò v. Italy, appl.no. 11339/85.
ECtHR, judgment of 22 April 1992, Vidal v. Belgium.
ECtHR, judgment of 9 June 1998, Teixeira de Castro v Portugal, appl. no. 25829/94.
ECtHR, judgment of 4 July 2002, Parris v Cyprus, appl.no. 56354/00.
ECtHR, judgment of 19 June 2003, Hulki Güneş v. Turkey, appl.no. 28490/95.
ECtHR, judgment of 3 April 2007, Copland v United Kingdom, appl. no. 62617/00.
ECtHR [GC], judgment of 4 December 2015, Roman Zakharov v Russia, appl.no. 47143/06.
ECtHR, Big Brother Watch and Others v. the United Kingdom, Press release, 13 September 2018.

Court of Justice of the European Union

CJEU, Judgment of 30 November 2016, Arkady Romanovich Rotenberg v. Council of the European Union, T-720/14.

8.3 Documents of European Organisations

European Commission

European Commission (EC), GREEN PAPER on obtaining evidence in criminal matters from one Member State to another and securing its admissibility, Brussels, 11.11.2009, COM (2009) 624 final.

Communication from the Commission to the European Parliament and the Council: An area of freedom, security and justice serving the citizen, COM (2009) 262.

European Commission (2016), Questionnaire on improving criminal justice in cyberspace - Summary of Responses.

European Commission, STAFF WORKING DOCUMENT, Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC, Accompanying the document - Proposal for a Regulation of the European Parliament and the Council on the protection of privacy and confidentiality in relation to electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, Brussels, 10.1.2017, SWD(2017) 5 final.

Non-paper from the Commission services, Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward, June 2017.

European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS,

Tackling Illegal Content Online Towards an enhanced responsibility of online platforms, COM (2017) 555 final, Brussels, 28.9.2017.

European Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C 2018) 1177 final.

European Commission (EC), COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD/2018/118 final - 2018/0108 (COD), Brussels, 17.04.18.

European Commission, The European Union Blockchain Observatory and Forum, Thematic Report, Blockchain and the GDPR, 16 October 2018.

Council of the European Union

Council of the European Union, Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

Conclusions of the Council of the European Union of 9 June 2016 on improving criminal justice in cyberspace, ST 9579/16.

Council of the European Union conclusions of 9 June 2016 on the European Judicial Cybercrime Network, 10025/16.210.

Council of the European Union, 7th round of Mutual Evaluations -The practical implementation and operation of European policies on prevention and combating cybercrime - Report on Luxembourg, Brussels, 2 May 2017, 7162/1/17 REV 1.

Article 29 Data Protection Working Party

Article 29 Data Protection Working Party, Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime, adopted on 22 March 2001, 5001/01/EN/Final WP 41.

Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014, 0829/14/EN WP216.

Statement of the Article 29 Data Protection Working Party, Data protection and privacy aspects of cross-border access to electronic evidence, Brussels, 29 November 2017.

European Union Agency for Network and Information Security (ENISA)

European Union Agency for Network and Information Security (ENISA), Identification and handling of electronic evidence –Handbook, document for teachers, September 2013.

European Union Agency for Network and Information Security (ENISA), Electronic evidence - a basic guide for First Responders Good practice material for CERT first responders, 2014.

European Union Agency for Network and Information Security (ENISA), Forensic analysis – Local Incident Response Handbook, Document for teachers, December 2016.

Other institutions, agencies and bodies
European Anti-Fraud Office (OLAF), Guidelines On Digital Forensic Procedures For OLAF Staff, 15 February 2016.

Council of the European Union, Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating Cybercrime" - Report on Cyprus, Brussels, 15 July 2016, 9892/1/16 REV 1.

European Parliament, Distributed Ledger Technology And Financial Markets, Briefing, November 2016.

European E-justice Portal - Evidence, https://e-justice.europa.eu/content_evidence-92-en.do (accessed September 10, 2018).

European Judicial Network (EJN), New rules on data protection for EU institutions agreed, 30 May 2018, available at: https://www.ejn-crimjust.europa.eu/ejn/NewsDetail.aspx?Id=609 (accessed September 12, 2018).

European Data Protection Board, Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b), adopted on 26 September 2018.

8.4 Documents of International Organisations

Council of Europe
Council of Europe, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, CETS 185.

Council of Europe, Status regarding Budapest Convention – The Netherlands, *coe.int*

Council of Europe, Data protection and Cybercrime Division, Electronic Evidence Guide, Strasbourg 3 February 2013.

Council of Europe, Electronic Evidence Guide, A basic guide for police officers, prosecutors and judges, Strasbourg, 15 December 2014.

Council of Europe, Enhanced international cooperation on cybercrime and electronic evidence: Towards a Protocol to the Budapest Convention, 2 November 2017.

Council of Europe, Enhanced international cooperation on cybercrime and electronic evidence: Towards a Protocol to the Budapest Convention, 19 March 2018.

Cybercrime Convention Committee
Council of Europe, European Committee on Crime problems (CDPC), Draft Explanatory Memorandum to the Draft Convention on Cybercrime, Strasbourg 14 February 2001.

Council of Europe, Cybercrime Convention Committee (T-CY), T-CY Guidance Note #3 Transborder access to data (Article 32), Strasbourg, 3 December 2014.

Council of Europe, Cybercrime Convention Committee (T-CY), Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final report of the T-CY Cloud Evidence Group, Strasbourg France, 16 September 2016.

Council of Europe, Cybercrime Convention Committee (T-CY), T-CY Guidance Note #10, Production orders for subscriber information (Article 18 Budapest Convention), Strasbourg 1 March 2017, T-CY (2015)16.

8.5 European Legislation

Council of Europe

Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5.

Council of Europe, *European Convention on Mutual Assistance in Criminal Matters*, ETS No.030, Strasbourg 12 June 1962.

Council of Europe, *Convention for the protection of individuals with regard to automatic processing of personal data* (ETS No. 108, 28.01.1981).

Council of Europe, *Recommendation No. R (87) 15*, 17 September 1987.

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

Council of Europe, *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Treaty Series-No. [223], Strasbourg, 10.10.2018.

European Union

The Schengen acquis - 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. 19–62.

Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperate on between national authorities responsible for the enforcement of consumer protection laws.

Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams.

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

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.

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.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257/73.

Regulation (EU) 2016/95 of the European Parliament and of the Council of 20 January 2016 repealing certain acts in the field of police cooperation and judicial cooperation in criminal matters, OJ L 26, 2.2.2016.

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

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.

8.6 Other sources

Anwar, H., Consensus Algorithms: The Root Of The Blockchain Technology, 25 August 2018, *101blockchains.com*

Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, March 2012.
Big Brother Watch, Police Access to Digital Evidence - The powers of the Police to examine digital devices and how forces are training staff, November 2017.

Blockchain and Digital Chain of Evidence, 13 March 2018, *Kinesense-vca.com*

Blockchain Bundesverband, Blockchain, Data Protection and the GDPR, 25 May 2018, *bundesblock.de*

Bonomi, S. et al. B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics, available at: https://arxiv.org/pdf/1807.10359.pdf (accessed October 22, 2018).

Commission Nationale de l'Informatique et des Libertés (CNIL), Blockchain et RGPD: quelles solutions pour un usage responsable en présence de données personnelles ?, 24 September 2018.

Commission Nationale de l'Informatique et des Libertés (CNIL), Premiers éléments d'analyse de la CNIL – Blockchain, September 2018.

Cooper, B., The Current State Of Blockchain Regulation, 30 May 2017, *mobilepaymentstoday.com*

Curran, B. What is Proof of Authority Consensus? Staking Your Identity on The Blockchain, 5 July 2018, *Blockonomi.com*

Cybersecurity Nexus, Overview of Digital Forensics, *infosecurityeurope.com*

CYBER-TRUST project, D3.1 Regulatory Framework Analysis, August 2018.

Dutch government, Senate approves legislative proposal on Computer Crime III, 26 June 2018, available at: https://www.government.nl/latest/news/2018/06/26/senate-approves-legislative-proposal-on-computer-crime-iii (accessed 30 October 2018).

EDRi, Cybercrime Convention -cross-border access to electronic evidence, 17 January 2017.

European Judicial Training Network (EJTN), Evidence And Proofs From The Perspective Of The European Court of Human Rights, *ejtn.eu*

EVIDENCE project (2016), European Informatics Data Exchange Framework for Courts and Evidence, D3.1 Overview of existing legal framework in the EU Member States.

EVIDENCE project, Final Report Summary (European Informatics Data Exchange Framework for Courts and Evidence), *cordis.europa.eu*

EVIDENCE Project, Horizon 2020-funded initiative from the European Commission to collect information concerning the handling of electronic evidence in European Union.

Forensic Science Regulator (2014), Codes of Practice and Conduct, Appendix Digital Forensic Services, Issue 1.

Hill, R., Boffins: Confusing distributed ledger tech definitions create 'unrealistic expectations' about what it can do - Report proposes tight conceptual DLT framework,14 August 2018, *Theregister.co.uk*

Italy - Country Wiki - Council Of Europe, available at: https://www.coe.int/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/cont (accessed September 09, 2018).

KPMG, Consensus Immutable agreement for the Internet of value, June 2016.

McBride, J., The case law of the European Court of Human Rights on evidentiary standards in criminal proceedings, European Union - Council of Europe joint project "Application of the European Convention on Human Rights and harmonisation of national legislation and judicial practice in line with European standards in Georgia".

McKinlay et al., Blockchain: Challenges And Legal Issues Of New Technology, 2 February 2018, *dlapiper.com*

Open Trading Network, UK Police — Blockchain solutions on the horizon, 3 December 2017, *medium.com*

Schulman, C., Legislation and legal frameworks on cybercrime and electronic evidence: Some comments on developments 2013 – 2018, United Nations Intergovernmental Expert Group on Cybercrime, Panel on legislation and legal frameworks, Vienna 3-5 April 2018.

Szabo, N. (1994), Smart contracts, available at: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (accessed 30 October 2018).

The Criminal Procedure Rules, Part 19 – Expert Evidence, October 2015 as amended April 2018.

UK Government Office for Science (2016), Distributed Ledger Technology – Beyond Blockchain, A report by the UK Government Chief Scientific Adviser.

