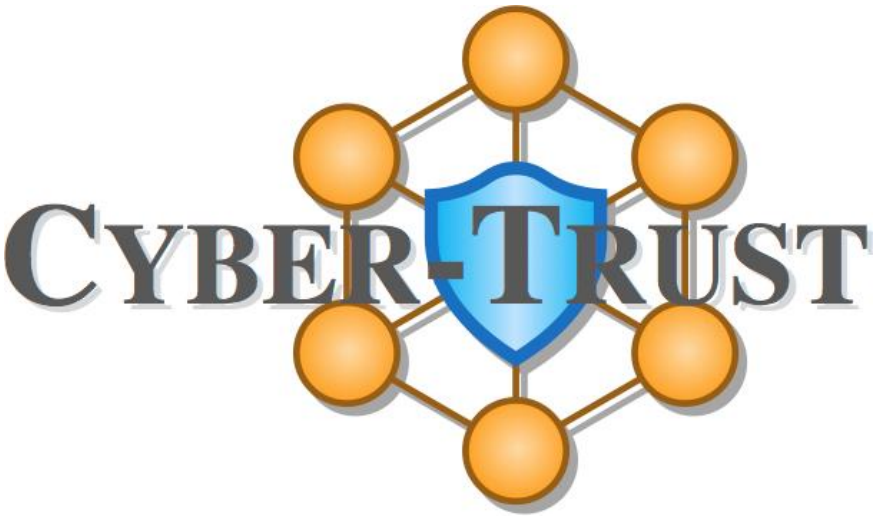
Ref. Ares(2019)18118 - 03/01/2019



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

D3.1 Regulatory framework analysis

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: 31/08/2018
Document Submission Date: 31/08/2018

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

Document Information

Deliverable number:	**D3.1**
Deliverable title:	Regulatory Framework Analysis
Deliverable version:	1.4
Work Package number:	3
Work Package title:	Legal issues: data protection and privacy
Due Date of delivery:	31 Aug 2018
Actual date of delivery:	31 Aug 2018
Dissemination level:	PU
Editors:	Olga Gkotsopoulou (VUB) Paul Quinn (VUB)
Contributors:	Nikolaos Kolokotronis (UoP) Kostas Limniotis (UoP)
Reviewers:	George Kokkinis (KEMEA) Dimitrios Kavalieros (KEMEA) Prof Steven Furnell (CSCAN) Dr Stavros Shiaeles (CSCAN)
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
0.1	29.07.18	VUB	1st draft
0.2	31.07.18	VUB	Internal feedback
0.3	07.08.18	VUB	Input by UoP
0.4	08.08.18	VUB	Input by UoP
0.5	16.08.18	VUB	Final draft after internal review
1.0	17.08.18	VUB	Submission of the final draft to reviewers
1.1	28.08.18	VUB	Feedback by KEMEA
1.2	29.08.18	VUB	Feedback by CSCAN: Section 8.1 added
1.3	31.08.18	VUB	Proofreading of the document Final version submitted to PC
1.4	10.12.2018	VUB	Updated version

Disclaimer: This Deliverable reflects only the authors' views, and the European Commission is not responsible for any use that may be made of the information it contains.

Copyright © Cyber-Trust Consortium. All rights reserved.

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
GC	Grand Chamber
GCC	Greek Criminal Code
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Computer Technologies
IoT	Internet of Things
ISP	Internet Service Provider
LEA	Law Enforcement Agency
M2M	Machine to Machine
MLA	Mutual Legal Assistance
NIS	Network and Information Security
No.	Number
OECD	Organization for Economic Cooperation and Development
OES	Operator of Essential Services
OJ/OJ L […]	Official Journal of the European Communities - Legislation
para.	Paragraph
PET	Privacy-enhancing technologies
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
UDHR	Universal Declaration of Human Rights
UN	United Nations
US/USA	United States of America
v	Versus
WP	Work Package

Copyright © Cyber-Trust Consortium. All rights reserved.

Contents

Copyright © Cyber-Trust Consortium. All rights reserved.

Copyright © Cyber-Trust Consortium. All rights reserved.

Copyright © Cyber-Trust Consortium. All rights reserved.

Copyright © Cyber-Trust Consortium. All rights reserved.

Executive Summary

Privacy in the context of Cyber-Trust

A recognition of the risks that surveillance practices in the context of cyber-threat intelligence gathering and sharing, as well as the use of new technologies for the detection and mitigation of cyberattacks and the storage of evidence, can create for privacy, is essential in Cyber-Trust project. This is so for several reasons to do with both what the Cyber-Trust project aims to achieve, as well as the Cyber-Trust prototype itself, during its creation and design phase but also in the case of a possible use after its release. Automated tools used for scraping data and profiling of devices offer a means for digital surveillance, which can interfere with individuals´ privacy in its various forms, in particular, due to the intrusiveness of the method and the enormity of the data being collected in combination with a false impression of anonymity online. Even in the case where no personal data are collected, digital surveillance activities may still exert psychological pressure upon individuals and may be capable of affecting or altering their behaviour.

Alleged interferences with personal privacy, however, are not always unacceptable. This includes potential uses in incidents relating to cybersecurity and elimination of cybercrime for which Cyber-Trust is intended. Depending on the severity of the interference with privacy and the purpose and the features of the tools used, the deployment of the Cyber-Trust system may be acceptable in most contexts, depending on a case-by-case assessment. The protection of privacy has to be weighed towards other prominent duties of the states related to the need to protect the life and property of individuals, to prevent, detect, prosecute or investigate criminal activity and to guarantee national security and critical infrastructure. The concept of proportionality, in a broader sense and the proportionality test, in a narrower sense, as introduced by the ECtHR case law, provide a way of judging when such interference may be acceptable.

The Importance of Data Protection to Cyber-Trust

Whenever the system collects and processes personal data, it will be necessary to comply with the existing data protection frameworks at national, European and international level. With respect to the Cyber-Trust project, the two main legislative initiatives that are likely to be of relevance are the General Data Protection Regulation (GDPR) and the Police and Criminal Justice Data Protection Directive (Directive 2016/680). The use of a Cyber-Trust prototype by law enforcement could be exempted from the field of application of the GDPR. Specifically, the Recital 19 excludes the application of the Regulation to personal data being used for police and criminal justice activities on the grounds of public security and public order. However, this kind of use may fall under the scope of Directive 2016/680. The requirements for the processing of personal data that falls within the scope of this Directive may depend upon the particularities of individual Member State law.

Cybercrime and Cybersecurity - Legal Frameworks

Cybersecurity and cybercrime are two highly interconnected topics. Even though there is no single definition for “cybercrime,” the term is used to describe various offences including conventional computer-based crimes, as well as network crimes. Within the EU and its Member States, several legislative and non-legislative efforts attempt to harmonize the legislative framework. Three instruments are being widely accepted and implemented: The Council of Europe Convention on Cybercrime, and in EU level, the Directive 2013/40/EU on attacks against information systems and the Directive 2016/1148/EU concerning measures for a high common level of security of networks and information systems. All three have influenced the way States regulate cyberthreats and cybercrimes, their prevention, detection, investigation, and prosecution, as well as their relevant cybersecurity policies and strategies. In most cases, cybercrimes are covered by Criminal Codes and Codes of Criminal Procedures of the Member States. However relevant provisions can also be found in various other national laws. In particular, tools used in the Cyber-Trust project, such as web crawlers, automated techniques for the profiling of IoT devices and packet inspection tools should be deployed in compliance with all the necessary safeguards and under the specific conditions described by those legal instruments.

Copyright © Cyber-Trust Consortium. All rights reserved.

Electronic evidence

The aim of the Cyber-Trust project is to develop a prototype that will not only be capable of detecting possible cyberthreats and contribute to their mitigation but also to provide material that could be used as evidence in criminal proceedings. In order to be able to make use of data in such a manner, the potentially evidentiary material will have to be collected, stored, and handled in a way that is not only consistent with laws concerning human rights and data protection, but also with rules concerning the handling of evidence in criminal proceedings. Failure to comply in any of the stages of the collection and handling could result in material which would be inadmissible for further investigation and criminal proceedings.

Rules concerning the admissibility of evidence are a matter of complex and highly sophisticated national legislation, which often does not address the issue of electronic evidence, as such but rather applies outdated legal schemes to it, by analogy. Therefore, it is not possible, at the moment, to present a single legal approach for the Cyber-Trust project that would be acceptable in all jurisdictions. However, the current legislative reform that takes place in European – led by the European Commission and the co-legislators, and in international level – mainly, led by the Convention on Cybercrime Committee (C-TY) - aims to simplify the existing processes and put in place further safeguards for individuals´ rights, establishing a more coherent environment for cooperation on law enforcement and judicial matters across EU Member States and other third countries.

Notwithstanding the differences in the various domestic laws, it will be important for the partners involved in the design of a Cyber-Trust prototype to follow some common principles, facilitating good practices with regards to the handling of evidence. Since not explicitly regulated, the use of Blockchain technologies for the storage of evidence could spark a vivid debate about its appropriateness in such a context, in terms of data protection and admissibility before a Court, as it will be discussed in detail in Deliverable 3.2.

Copyright © Cyber-Trust Consortium. All rights reserved.

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, on the basis of blockchain and machine learning tools.

By establishing an innovative cyber-threat intelligence gathering, detection, and mitigation platform, as well as, by performing high-quality interdisciplinary research in critical 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 (zero-day vulnerability discovery and sharing), b. cyber-attack detection and mitigation (IoT device tampering and network/DoS attacks), and c. distributed ledger technologies.

In specific, it aims to create a new paradigm for the next generation cyber-security systems, especially suited for the IoT, to quickly detect and mitigate complexed cyber-attacks, to deliver advanced solutions for the collection and use of forensic information, and to develop and implement data protection by Design and by Default models.

1.2 Purpose of the Document

The present deliverable (D3.1), the first 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 platform design, and conduct a Data Protection Impact Assessment (DPIA), in accordance with Article 35 of the EU General Data Protection Regulation (GDPR).

Even though the Cyber-Trust consortium will attempt, during the research phase, to avoid the collection and processing of personal data, it acknowledges that where such processing becomes necessary, the partners will plan accordingly in order to ensure that any legal and ethical risks are minimised, by implementing all necessary and appropriate technical and organisational measures. It should also be noted that D3.1 is not to be seen as a contextual legal analysis of the Cyber-Trust systems and processes, but instead as a broader overview of the main governing legal regimes and principles. A more in-depth legal analysis will be the subject of the next four deliverables included in the WP3, namely D3.2, D3.3, D3.4, and D3.5.

Thus, the deliverable D3.1 will offer oversight of the legal framework that is applicable to the Cyber-Trust project and will be considered as a compass for the creation of suitable technical measures that are meeting all the legal requirements, mirroring the content of task T3.1. The input of the present deliverable will be used for the adoption of proper practices and technical measures concerning the data collection from both clear net/deep web and IoT devices, including techniques related to the use of IP headers and TCP dumps. More specifically, it will be integrated into the implementation of the tasks T5.1 and T6.1 on cyber-threat intelligence information gathering and privacy-preserving device profiling respectively. Both tasks will be necessarily restrained from what is legally and ethically permissible in terms of the various forms of personal data collection that may be practised within the Cyber-Trust project, where strictly necessary. Lastly, by drawing an outline of the main areas of applicable law, D3.1 will provide Cyber-Trust partners with a set of key notions that will serve as a reference to assess the impact of the work of the project with respect to the relevant identified legal issues.

1.3 Scope and Intended Audience

The analysis of the regulatory framework will focus on the main instruments of international and European law, insofar as they concern the legal framework within the EU and its Member States. Whenever the relevant legislative initiatives take legal effect only under the condition of their transposition into domestic law, brief overviews of the legal systems in the states where the technical partners have their main establishment, as described in the official Proposal of the project, i.e., Cyprus, Greece, Italy, Luxembourg, The Netherlands and the United Kingdom, are provided.

Copyright © Cyber-Trust Consortium. All rights reserved.

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 Document

The deliverable is divided into four parts: Part A: Privacy, consisting of Sections Two and Three; Part B: Data Protection, consisting of Sections Four and Five; Part C: Cybercrime and Cybersecurity, consisting of Section Six and Part D: Electronic (or digital) evidence, consisting of Section Seven.

As Cyber-Trust constitutes what could be amounted to a system of indirect digital surveillance, monitoring, and profiling, it engages in privacy issues on different levels. Part A will expound upon the ethical aspects of privacy which relate to the Cyber-Trust system, with Section Two examining why notions of privacy and the ethics of internet research must be taken into consideration throughout the duration of the project. Section Three will evaluate these concepts against the countervailing principle of security and in particular, cybersecurity, while exploring how these ethical principles of privacy are reflected in the European legal framework in which Cyber-Trust will operate. These concepts should be seen as going beyond mere personal data, and largely are relevant even in circumstances where no personal data are processed.

Part B concerns the legal frameworks that are likely to be relevant to two main components of the system, detection and profiling on the one hand, and storage of evidence in a Blockchain on the other. First, Section Four will examine the potential impact of European data protection law on the Cyber-Trust project. As the most important manifestation of the notion of privacy in an informational sense referred to in Part A, this regime is concerned with the protection of the informational notion of privacy – that is, personal data. Section Five will explore the laws and regulations that are likely to be applicable to the Cyber-Trust project relating to the creation and design of the Cyber-Trust platform, as well as its release as a prototype and will provide guidelines for their proper implementation in the project context.

Part C will shift focus to the primary aim of the Cyber-Trust project, which is cybersecurity and mitigation of cybercrime. Section Six will detail the relevant laws and regulations concerning cybercrime and the obligation of states and other involved organisations to implement measures for protecting themselves and individuals against cyber attacks, both at European and domestic level. Only the legislation of a selected number of Member States which are relevant for the operations of the Cyber-Trust project will be presented, although, given the globality of the internet, the global aspect of the project is to be taken into consideration.

Part D and respectively Section Seven will provide an initial overview of the legislation in European and national level, concerning the use of electronic evidence for the investigation and prosecution of cybercrimes. Section Seven will also include a first brief analysis of the use of Distributed Ledger Technologies (DLT) for the storage of evidence for law enforcement matters. However, the overview will be kept short, as this subject is going to be addressed in detail in Deliverable D3.2.

Copyright © Cyber-Trust Consortium. All rights reserved.

Part A – Privacy

2. Ethical considerations of privacy

The digital age is characterised by the widespread use of computers, the internet, and numerous technological media, making the bulk data collection reaching globally unprecedented levels. Extracted from social networks, images, satellites, literature, sensors, the web and smart devices, everything we do, did or will do, leaves massive traces of activity, which will continue to exist even after our death, moving the world swiftly towards a state of complete "datafication."[1] This information, deliberately or not, is being increasingly deposed in various data repositories, belonging to the private or public sector, serves different purposes and constitutes an extensive pool of knowledge. This knowledge, in turn, is either used raw in its primary form, facilitating, for instance, the performance of a contract; or handled to generate more knowledge. Thus, very often, the raw data and the subsequent knowledge it provides is widely used for business and management purposes, in research and science, health care, policy-making and law enforcement, but as well in digital surveillance, micro-targeting, and behavioural advertising.

Of course, not all of these data are personal. Nevertheless, depending on the circumstances, a big or small amount of it is personal data or, might have been at some stage of the processing. And of course, it goes without saying that collection of data through various means is not a new or unfamiliar concept for most societies, taking into account that "humans, unlike other entities, are inherently self-documenting."[2] However, what is striking is the -without precedent- high volume and variety of the data being collected from divergent sources in combination with the high speed of the processing, putting the data in the hands of numerous actors for different purposes.

Thus, despite its undoubtedly multiple benefits, the digital age poses significant challenges to privacy and calls for more stringent cybersecurity strategies. In 2013, the Snowden´s revelations about the alleged operation of large-scale surveillance programmes by state intelligence agencies sparked severe concerns around the triptych of privacy, surveillance, and security. This section will focus on these three concepts from an ethical and legal perspective, introducing essential principles that are likely *inter alia* to have an impact upon the development and use of a Cyber-Trust prototype.

Some first references to the correlation between big data[3] and privacy appear as early as in 1971,[4] in the *Arthur Miller´*s study "Assault on privacy," where abuses of large-scale record-keeping systems are presented.[5] Nowadays, the concepts of both privacy and security are well-established in every modern pluralist democratic society. Without security nor privacy, freedom and human dignity become impossible. In discussing privacy in the context of public order and security, it is consequently necessary to make clear that effective privacy requires an adequate state of security in society. Likewise, by ensuring that society is as secure as possible, it is important to realize and maintain individual privacy given that a life without adequate privacy, even in an environment that is secure from crime and disorder would not be bearable either.[6]

[1] Mai, J-E, Big data privacy: The datafication of personal information, The Information Society, 32, 3, (192), (2016).
[2] ASU Alumni (2018), Why are human so obsessed with self-documenting?, asu.edu
[3] The Article 29 Data Protection Working Party uses the following definition to describe big data: "Big data refers to the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organizations, which are then extensively analyzed (hence the name: analytics) using computer algorithms. Big data can be used to identify more general trends and correlations but it can also be processed in order to directly affect individuals." See: Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, adopted on 2 April 2013, WP203.
[4] Part A includes references to previous work undertaken by the editor, at: Gkotsopoulou, O. (2015), How big is your privacy in a big data world?, unpublished manuscript, Europa Universität Viadrina.
[5] Miller, A. R. (1971). The assault on privacy: Computers, data banks, and dossiers. Ann Arbor: University of Michigan Press.
[6] Solove, D. J. (2011). Nothing to hide: The false tradeoff between privacy and security. New Haven [Conn.]: Yale University Press.

Copyright © Cyber-Trust Consortium. All rights reserved.

Statements made by big corporations and their representatives often endorse the nothing-to-hide argument and consider privacy an outdated concept.[7] On the other hand, "[t]he very existence of an internationally recognised right to privacy", had argued the former Secretary-General of the United Nations, "presupposes agreement that there are certain areas of the individual's life that are outside the concern of either governmental authorities or the general public, areas which may vary in size from country to country, but which do possess a common central core."[8]

2.1 The concept of privacy in the digital age

Privacy is a term that is everywhere in our informational society. Individuals seek it, business and governments claim to respect it. A plethora of similar terms is used interchangeably to refer to privacy, including "private life," "private sphere," "intimacy" and "secrecy," causing ambiguity and complexity.[9] Yet privacy is a concept without a single commonly accepted definition.[10] Whereas *Thomson* and *Scanlon* refer to a rights-based concept, other legal theorists and philosophers approach privacy as an interest-based one.[11] Consequently, some scholars, in order to overcome the hurdles of such a lack of collective agreement, decided to rely upon a more contextual and relativistic ground where privacy is defined in accordance with the context it is discussed within. In that approach, definitions vary depending on the context, culture, and society. Some countries follow a narrow interpretation of privacy, others a broader one. However, in most societies, privacy is often seen as the drawn line which indicates how far someone can intrude into another individual's personal life.[12] Indeed, one major discussion about privacy, in particular, triggered by the rise of information technology and the internet, is that of privacy in the public realm and privacy in the private realm, which according to *Nissenbaum,* in its core, could also be seen as a contrast between public realm and personal.[13]

Westin discussed privacy and freedom in various concepts and created a debate framework, conceptualizing four states of privacy - solitude, anonymity, reserve, and intimacy – already in 1967.[14] *Solove*, on the other hand, argued that the conceptions of privacy could be grouped in six categories:[15] a) "the right to be let alone" – *Samuel Warren* and *Louis Brandeis'*s formulation for the right to privacy; [16] b) "limited access to the self"; c) "secrecy"; d) "control over personal information"; e) "personhood"; and f) "intimacy".[17] To the contrary, *Rössler* introduced three dimensions of privacy:[18] a) decisional privacy, which is necessary for individual autonomy; b) informational privacy, i.e., control over information relating to a person; c) local privacy, i.e., privacy of the household, of one's flat or room and hence privacy of objects. *Banisar and Davies* came up with another similar, yet different categorisation as follows:[19] a) informational privacy, concerning the collection and handling of personal data; b) bodily privacy, with regards to the protection of a person's physical integrity against invasive procedures, such as clinical trials; c) privacy of communications, covering

[7] Ibid.
[8] American Civil Liberties Union (2014), "Privacy Rights in the Digital Age, A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights: A Draft Report and General Comment by the American Civil Liberties Union", p.14.
[9] Tavani, T. H. (2009), Informational Privacy: Concepts, Theories, and Controversies in: The Handbook of information and Computer Ethics.
[10] Ibid.
[11] Ibid. See also: Scanlon, T. (1975), Thomson on Privacy. Philosophy and Public Affairs 4.4: 315-322.
[12] Ibid.
[13] Nissenbaum, H. (1997), Toward an Approach to Privacy in Public: Challenges of Information Technology, Ethics & Behavior, 7:3, 207-219.
[14] Westin, A. F. (1967), Privacy and freedom. New York: Atheneum.
[15] Solove, D. J. (2008), Understanding privacy. Cambridge, Mass: Harvard University Press, p.13.
[16] Warren, S.D. & Brandeis, L.D. (1890), The Right to Privacy, Harvard Law Review, Vol. 4, No. 5, pp. 193-220.
[17] Quinn, P. (2016), Deliverable D2.1, FORENSOR.
[18] Roessler, B. (2006), New Ways of Thinking about Privacy. In Anne Philips Bonnie Honig & John Dryzek (eds.), Oxford Handbook of Political Theory. Oxford University Press. pp. 694-713.
[19] Banisar, D. & Davies, S. (1999), Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments, 18 J. Marshall J. Computer & Info. L. 1.

Copyright © Cyber-Trust Consortium. All rights reserved.

the security and confidentiality of every form of communication; and d) territorial privacy, concerning protection of the domestic and other environments, such as the workplace.

*Nissenbaum´*s conception of privacy in public, including cyberspace that extends to consider the processing of all information, including information gathering in a so-called public realm should be taken into account when perceiving privacy in the digital age.[20] This conception addresses two erroneous assumptions; first that there is a realm of public information related to individuals where no privacy norms apply at all, and therefore this information is "up for grabs" by anyone; and second, that the aggregation of information does not violate privacy given that its parts, collected separately, did not violate privacy.[21]

2.2 Personal autonomy in relation to privacy

One common link between all those various conceptions of privacy is the idea of "autonomy," i.e., that individuals be left as much as possible to define themselves. *Westin* defines privacy as the desire of people to choose freely under which conditions and to what extent, they want to expose themselves to others.[22] In *Joseph et al.*, it is argued that privacy constitutes "freedom from unwarranted and unreasonable intrusion into activities […] belonging to the realm of individual autonomy".[23] "Individual autonomy" in its turn refers to the field of action that does not touch upon the liberty of others, where a person can shape one's life according to one's own wishes and expectations[24] and includes as well interaction with other persons, such as private communications. *Bloustein* considers privacy as an inherent interest of the inviolate human personality, the individual's independence, dignity, and integrity.[25] The American jurist *Louis Brandeis* described privacy as "the most fundamental of all rights cherished by a free people," whereas *Volio* underlines that "in one sense, all human rights are aspects of the right to privacy."[26]

The concept of personal autonomy and its relation to privacy is *inter alia* often reflected in the jurisprudence of the European Court of Human Rights (hereinafter ECtHR) under Article 8 of the European Convention on Human Rights (hereinafter ECHR),[27] which is related to the protection of private and family life. In the ECtHR case law, personal autonomy which falls under the scope of the right to respect for private life, primarily observed as an aspect of the right to physical and social identity and defined as "the ability to conduct life in a manner of one's own choosing", is used to offer a more contextual interpretation of the right to privacy.[28] It is worthy to mention that the notion of personal autonomy holds a special place in the Strasbourg Court case law and underlies the interpretation of all Convention guarantees[29], and not only those of the specific article.[30]

This personal autonomy, provided in the concept of privacy, may suffer physical intrusions or psychological pressures and influences from outside sources, which depending on the context, could impose obstacles to

[20] Nissenbaum, H. (1997).
[21] Ibid.
[22] Westin, A. F. (1967).
[23] Joseph, S, Schultz, J. & Castan, M. (2004), The International Covenant on Civil and Political Rights: Cases, Materials and Commentary, Oxford University Press.
[24] For more on the notion of the "autonomous self", see Cohen, J. (2013), What Privacy is for, Harvard Law Review 126(7), 1904-1933, p. 1907.
[25] Bloustein, E. (1984), Privacy as an aspect of human dignity: An answer to Dean Prosser. In F. Schoeman (Ed.), Philosophical Dimensions of Privacy: An Anthology (pp. 156-202). Cambridge: Cambridge University Press.
[26] Volio, F (1981), Legal Personality, Privacy and the Family in Henkin (ed) The International Bill of Rights (Colombia University Press).
[27] 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.
[28] Koffeman, N.R. (2010), (The right to) personal autonomy in the case law of the European Court of Human Rights, Leiden, p.16.
[29] The Court continued that therefore this notion must be seen as "an essential corollary of the individual's freedom of choice implicit in Article 11 and confirmation of the importance of the negative aspect of that provision.' ECtHR [GC] judgment of 11 January 2006, Sørensen and Rasmussen v. Denmark, appl. nos. 52562/99 and 52620/99, para. 54.
[30] ECtHR judgment of 27 April 2010, Ciubotaru v. Moldova, appl. no. 27138/04, para. 49; ECtHR judgment of 8 January 2009, Schlumpf v. Switzerland, appl. no. 29002/06, para. 100. See also ECtHR judgment of 15 January 2009, Reklos and Davourlis v. Greece, appl. no. 1234/05, para 39.

Copyright © Cyber-Trust Consortium. All rights reserved.

a person´s development or cause alterations to their behaviour. Examples of such pressures could involve intrusion into individuals' home or private spaces, interference with the freedom to choose one's own form of education and attacks on ideas or beliefs that individuals may hold and express. *Westin* classified the relevant threats in terms of physical, psychological and data surveillance. The latter has obvious relevance for the Cyber-Trust project.

"[State's effectiveness] in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance. The State now has a greater capability to conduct simultaneous, invasive, targeted, and broad-scale surveillance than ever before. In other words, the technological platforms upon which global, political, economic, and social life are increasingly reliant are not only vulnerable to mass surveillance; they may actually facilitate it."[31] Surveillance activities, however, are not only deployed by states and are not only passive activities collecting information that may relate to persons but are also capable of influencing individuals and are closely related to the exercise of other fundamental rights and freedoms, such as the freedoms of thought and expression, movement and association.[32] [33] On that end, the UN Special Rapporteur on the protection and promotion of the right to freedom of expression and opinion, *Frank La Rue*, had observed that insufficient protection of privacy may have "a chilling effect" on other rights.[34]

2.2.1 The notion of informational privacy

In the computer ethics literature, there are three major theories around informational privacy.[35] First, the restricted access theory entails that one has informational privacy when she is able to limit or restrict others from access information about herself. Second, according to the control theory, privacy is directly linked to one´s having control over information about oneself. And a third theory comes from a mixed perception of the two aforementioned theories, in conjunction with limited control of the data subject over her data.[36] Notions of informational privacy may give rise to legal approaches providing control over or restricted access to images, communications, health information, and many other aspects. It is entirely possible that where the data protection framework does not apply, other legal and ethical approaches linked to privacy may still be relevant. As section 3.4.2 of this document discusses, this involves other privacy approaches and doctrines including notably those developed by the ECtHR under Article 8 ECHR.

Like most other conceptions of privacy, informational privacy is often connected to the concept of autonomy given that individuals may often change their behaviour as a result of the information about them that is known to others. Harms to privacy in the informational sense usually thus refer to instances where information concerning individuals has been collected, used or made public contrary to the wishes of those concerned. The notion of informational privacy can play an essential role in the Cyber-Trust project, in particular concerning data scraping from the clear net and the deep web, as well as in the storage of digital evidence in the blockchain and the enforcement of the data subject´s rights.

2.2.2 Data Protection as an aspect of informational privacy

Data protection started to be discussed only in the 1960s as part of the political agendas of advanced industrial states.[37] It was the outcome of the fast development and application of IT with regard to the

[31] U.N. Human Rights Council, The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights, OHCHR, U.N. Doc. A/HRC/27/37 (June 30, 2014) [hereinafter The Right to Privacy in the Digital Age].

[32] ECtHR judgment of 27 April 2010, Vördur Olafsson v. Iceland, appl. no. 20161/06, para. 46.

[33] Council of Europe, Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, home and correspondence, updated on 31 August 2018, p.37.

[34] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, A/HRC/23/40, p.7.

[35] Tavani, T. H. (2009), p.143.

[36] Ibid, p. 145.

[37] Smith, H.J., Dinev, T. and Xu, H. "Information Privacy Research: An Interdisciplinary Review," MIS Quarterly Vol.35 (4) (December 2011), pp. 989–1015.

Copyright © Cyber-Trust Consortium. All rights reserved.

collection and handling of personal information.[38] [39] The Land of Hessen in Germany adopted the first data protection laws in 1970. It was then followed by Sweden, the United States, and France. [40] [41] [42] Later on, data protection was included in the Council of Europe (CoE) 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (hereinafter Convention 108)[43] and the Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Trans-border Data.[44] These two documents had a significant impact on the relevant legislations which were from then on enacted all over the world concerning data protection.[45]

Data protection approaches lay out rules and conditions for the processing of personal data, and therefore they apply only in cases where personal data are involved. In contrast, data protection law does not apply where the processed data are not personal.[46] It is apparent that there is a common overlapping segment between privacy and data protection. However, their scopes are different, and the scope of data protection covers personal data only in an indirect way in relation to the private sphere.[47] Therefore, data protection is linked to privacy in that it can minimise the chances for personal data misuse and the consequent harms to individual autonomy and human dignity. Afore most, data protection principles, putting in place a system of checks and balances, can be engaged even where there is no demonstrable harm to individual privacy.[48] That observation is relevant for the Cyber-Trust partners who may process personal data, as it means that breaches of data protection principles and rules can occur even where no individual has complained of harms to his or her privacy because such infringement is not necessary for data protection rules to be triggered.

In the U.S.A. and the other Member States of the Inter-American Convention on Human Rights, there is no explicit differentiation between privacy and data protection. Often, there is a tendency both in literature and in legislation to deal with the right to data protection as a subset of the right to privacy.[49] [50] For instance, the Strasbourg Court has interpreted Article 8 European Convention on Human Rights, as if the right to data protection is encompassed in the right to private life.[51] Nevertheless, there is indeed a distinction established in Europe, in the EU Charter of Fundamental Rights[52] (hereinafter, EU Charter, CFR or EUCFR),[53] reflecting

[38] Bennett, C. J., "Regulating Privacy: Data Protection and Public Policy in Europe and the United States" (Ithaca: Cornell University press, 1992). p.2.

[39] Banisar, D. and Davies, S. (1999), "Global trends in privacy protection: An international survey of privacy, data protection and surveillance laws and developments," in: John Marshall Journal of Information and Technology and Privacy Law, Vol.18(1), Fall 1999.

[40] Ibid.

[41] See: Sietmann, R., "East German cancer data: a benefit of big brother?" in: Science Vol. 252 (5008), 17 May 1991, p. 915.

[42] Greenleaf, G., "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories" (September 10, 2013). (2014) 23(1) in: Journal of Law, Information & Science, Special Edition: Privacy in the Social Networking World.; UNSW Law Research Paper No. 2013-40.

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

[44] Organisation for Economic Cooperation and Development (OECD), Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data, 23 September 1980.

[45] Banisar, D. and Davies, S. (1999).

[46] Kokott, J. and Sobotta, C. (2013), The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR, in: International Data Privacy Law Vol.3 (4), pp.222–228.

[47] Friedewald, M. (Ed.), Burgess, J. (Ed.), Čas, J. (Ed.), Bellanova, R. (Ed.), Peissl, W. (Ed.). (2017), Surveillance, Privacy and Security, London: Routledge.

[48] Quinn, P. (2016).

[49] Lynskey, O. (2014), Deconstructing data protection: the added-value of a right to data protection in the EU legal order in International and Comparative Law Quarterly Vol.63, pp 569-597, p.570.

[50] Kokott, J. and Sobotta, C. (2013).

[51] See, eg, ECtHR, Amann v Switzerland, no. 27798/95, ECHR 2000-II, para. 65, Rotaru v Romania [GC] App no 28341/95, ECHR 2000-V, para. 43.

[52] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

[53] i.e. Article 7 and Article 8.

Copyright © Cyber-Trust Consortium. All rights reserved.

upon the General Data Protection Regulation[54] (hereinafter, GDPR or The Regulation) and the e-Privacy Directive.[55] [56] While Article 7 of the Charter protects the right to private life, Article 8 of the Charter addresses specifically the fundamental right to the protection of personal data.[57] In other words, the EU Charter deals with privacy and data protection as two separate rights which are not synonymous, while the Council of Europe in the ECHR deals with them as one in the text but distinguishes them in its case law, as seen below.[58] The failure in reaching a convincing rationale for the inclusion of an explicit right to data protection in the EU Charter created a lively debate among scholars for its potential justification. It has been suggested, for instance, that the Charter's right to data protection was introduced in order to boost the fundamental rights dimension of the Data Protection Directive, a former specific legal initiative of the EU, repealed by GDPR[59] or to cover gaps observed in it.[60] [61] Another explanation about this differentiation could be found in the way the article of the EU Charter about data protection is connected with strong ties to other human rights instruments which deal with the right to privacy, aiming to clarify its scope, specifically speaking Article 8 of the ECHR and the case law of ECtHR, as well as the Article 17 ICCPR and the General Comment No.16, the Article 12 UDHR and the Guidelines for the Regulation of Computerized Personal Data Files, adopted by the United Nations General Assembly in 1990.[62]

A separate right of data protection offers additional, distinct benefits for individuals, since the latter promotes the individual's right to personality, creating a concept of a further right to "informational self-determination" when it comes to technological innovations and data processing, as developed in the decisions Klass,[63] Malone,[64] Leander[65] and Huvig[66] of ECtHR.[67] [68] In this case, the collection, storage and processing of personal information by state authorities may constitute an interference with the right enshrined in the first paragraph of Article 8.[69] Nevertheless, these two rights are distinct both from a scope

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

[55] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47.

[56] CJEU, Case 136/79 National Panasonic v Commission [1980] ECR 2033, paras 17 et seq., and Case C-62/90 Commission v Germany [1992] ECR I-2575, para. 23.

[57] EU Network of independent experts on fundamental rights, Commentary on the European Charter of the Fundamental Rights of the European Union, June 2006, p.90-91.

[58] Kokott, J. and Sobotta, C. (2013): "In contrast, Article 8 of the Charter not only distinguishes data protection from privacy, but also lays down some specific guarantees in paragraphs 2 and 3…"

[59] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995 P. 0031 – 0050.

[60] Kuner, C., The European Union and the Search for an International Data Protection Framework, in: Groningen Journal of International Law, vol.2, ed.1: Privacy in International Law.

[61] Lynskey, O. (2014), p.570.

[62] EU Network of independent experts on fundamental rights (2006), p.90.

[63] Klass and others v Federal Republic of Germany, European Court of Human Rights [ECtHR], A/28, App.no.1979-80, 2 EHRR 214, 6 September 1978.

[64] Malone v. The United Kingdom, Judgment, European Court of Human Rights [ECtHR] A/82, App.no.8691/79, 2 August 1984.

[65] Leander v Sweden, Merits, European Court of Human Rights [ECtHR] App no 9248/81, A/116, (1987) 9 EHRR 433, IHRL 69 (ECHR 1987), 26th March 1987.

[66] Huvig and Huvig-Sylvestre v France, Merits, European Court of Human Rights [ECtHR], A/176-B App No 11105/84, (1990) 1 EHRR 528, IHRL 96 (ECHR 1990), 24th April 1990.

[67] This notion was referred to for the first time by the CJEU in the Opinion of Advocate General Cruz Villalón in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger delivered 12 December 2013 ECR [2013] I-0000.

[68] Lynskey, O. (2014), p.572.

[69] Bygrave, L. (1998), Data Protection pursuant to the Right to Privacy in Human Rights Treaties," International Journal of Law and Information Technology Vol.6(3), pp. 247–284, p.28.

Copyright © Cyber-Trust Consortium. All rights reserved.

and protection perspective,[70] mainly because the right to data protection provides individuals with more rights over data than the right to privacy and more specific protection over the new risks being imposed in the age of massive digital surveillance.[71] For instance, the additional rights that data protection grants to individuals, such as the right to data portability and the right to better determine how their data are processed, by whom and for what specific purposes as well as the right to object their accuracy, equip the individuals with better control over their personal data.[72] [73]

2.3 The Ethics of Internet Research and its relation to privacy

Internet Research Ethics could be defined as follows: "the analysis of ethical issues and application of research ethics principles pertaining to research conducted on the Internet".[74] Internet-enabled studies are used for the collection of information via online tools or specialised software, e.g. by examining activities on online environments or exploring publicly available online databases or repositories.[75] With the emergence of the Internet of Things (IoT), a global network connecting physical and virtual objects, by exploiting sensorially captured data and apparatus for communication and localisation, the opportunities for internet- and network-based research have increased exponentially.[76]

With respect to the Cyber-Trust project, of relevance is what could be defined as "research aiming to study information that is already available on or via the Internet without direct interaction with human subjects (harvesting, mining, profiling, scraping, observation or recording of otherwise-existing data sets, chat room interactions, blogs, social media postings, etc.)".[77] Thus, the internet can be seen both as a research tool and a research venue.[78] As a tool, internet research is facilitated by search engines, databases, and repositories, while possible venues could be places such as conversation applications, community platforms, news fora, blogs, etc.[79]

Researchers who conduct studies based on data collected from online public fora or social media, often bring the argument that subjects cannot have a reasonable expectation for privacy in the online enviroment since nearly all online interactions are regularly monitored by websites, service providers and other parties.[80] However, average internet users seem to lack understanding of how their activities are tracked, and are unaware of the related privacy practices and policies of the websites they visit or the devices they use.[81] This unclear distinction between private and public in the virtual ambience, as perceived by users, suggests researchers must assess *a priori* the type of social norms and relations governing an online space before making assumptions about the "publicness" of information shared within.[82] Such ambiguity could pose additional challenges to address privacy in an online or networked environment in the Cyber-Trust project.

[70] González Fuster, G., (2014), The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer International Publishing.

[71] Lynskey, O. (2014), p.572.

[72] Ibid, p.573.

[73] Special reference should be made to the right to object to automated individual decisions, the right to object due to the data subject's particular situation and the right to object the accuracy of information, which are specifically protected by the regulations of EU and CoE.

[74] Buchanan, E. A. and Zimmer, M. (2018), Internet Research Ethics, The Stanford Encyclopedia of Philosophy (Spring 2018 Edition), Edward N. Zalta (ed.).

[75] Ibid.

[76] Popescul, D. and Georgescu, M. (2013), Internet of Things – Some ethical issues, researchgate.net

[77] Buchanan, E. A. and Zimmer, M. (2018).

[78] Ibid.

[79] Ibid.

[80] van Dijck, J. (2014), Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society 12(2): 197-208, p.202.

[81] Milne, G. R. and Culnan, M.J. (2004), Strategies for Reducing Online Privacy Risks: Why Consumers Read (or don't read) Online Privacy Notices, Journal of Interactive Marketing, 18(3): 15–29.

[82] Rosenberg, A., 2010, "Virtual World Research Ethics and the Private/Public Distinction," International Journal of Internet Research Ethics, 3(1): 23–37. "Researchers could also argue that no consent is required due to the fact that the information is publicly available. In the case of the Facebook emotional contagion experiment, the lack of obtaining consent was initially tackled under the impression that the research had been carried out ´under Facebook's extensive

Copyright © Cyber-Trust Consortium. All rights reserved.

As a result, it is difficult to understand with certainty what the user's intention is when posting an item onto a platform.[83] Is her intention to make it visible to only a small circle of friends, but she failed to adjust the privacy settings accordingly? Or, the information might have previously been restricted to only certain friends, but a change in the technical platform enlarged the intended audience? Or, data was meant to be restricted to only a specific crowd, i.e. the subscribed users of a specific platform or community? Or, what if the data was copied from a restricted-access platform and reproduced in other open platforms by third persons? The extensive scraping of fora irrespective of who conducts the research – individual researcher, public or private organisation - poses risks to privacy in the broad sense, but also privacy in its informational conception, especially taking into account that social networks constitute a complex environment of socio-technical interactions, where understanding users´ intentions would require a case-by-case assessment, which under normal circumstances, is not likely.[84]

Another issue in the cases of wholesale scraping is that of the perception of anonymity.[85] *La Rue* argues that the right to privacy is fundamental for individuals to express themselves freely, emphasising on the fact that people are more willing to express themselves concerning controversial topics in public spheres when they can do that anonymously.[86] Hence, individuals may be discouraged to engage in communications, if they cannot be assured about the privacy of them.[87] [88] Internet serves both the purpose of communication and a sense of non-direct exposure since users have the opportunity to use public fora, where they do not have to reveal their offline identities. This is the case, in particular in the deep web, but similarly in the surface web. One problem in this area is that the user may assume that her computer-mediated or online activities are anonymous. In fact, the impression that one is anonymous online is widespread, even though one´s activities may be relatively easily monitored and identifiable by researchers and state authorities[89]. The user in such a case presumably desires anonymity as a way of ensuring privacy. Given that a user presumably desires anonymity and privacy, ethical issues may arise if deliberate deceptive practices encourage such mistaken presumptions about anonymity and privacy, especially in contexts of unwanted exposure or intrusive monitoring.[90]

terms of service´". See: Hill, K., 2014. Facebook Added 'Research' To User Agreement 4 Months After Emotion Manipulation Study, Forbes.com.

[83] Acquisti, A. and Gross, R. (2006), Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, Proceedings of the 6th Workshop on Privacy Enhancing Technologies, 4258: pp. 36–58.

[84] Buchanan, E. A. and Zimmer, M. (2018).

[85] van Dijck, J. (2014), p.202.

[86] "The same conclusion has been drawn by President Obama's Review Group on Intelligence and Communications Technologies, which argued that "if people are fearful that their conversations are being monitored, expressions of doubt about or opposition to current policies and leaders may be chilled, and the democratic process itself may be compromised."

[87] The European Union Advocate-General in Digital Rights Ireland Ltd v. The Minister for Communications, Marine and Natural Resources, brought up the same argument.

[88] UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Addendum, Communications to and from Governments, 16 May 2011, A/HRC/17/27: "As such, legitimate types of information which may be restricted include child pornography (to protect the rights of children), hate speech (to protect the rights of affected communities), defamation (to protect the rights and reputation of others against unwarranted attacks), direct and public incitement to commit genocide (to protect the rights of others), and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (to protect the rights of others, such as the right to life). However, in many instances, States restrict, control, manipulate and censor content disseminated via the Internet without any legal basis, or on the basis of broad and ambiguous laws, without justifying the purpose of such actions; and/or in a manner that is clearly unnecessary and/or disproportionate to achieving the intended aim, as explored in the following sections."

[89] Wallace, K.A. (1999), Ethics and Information Technology 1: 21, Kluwer Academic Publishers.

[90] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

The importance of seeking and receiving information online, without being targeted or monitored cannot be doubted.[91] [92] When a state or private actors monitor and collect vast amounts of information about individuals, this can constitute not only a violation of their right to privacy but also a violation of their right to free expression and an unbearable hassle for the free flow of information and ideas.[93] [94] In this regard, EU, as well as domestic law, often refer directly to the protection from interference with "correspondence", a term that should be interpreted broadly, including all forms of communication, both online and offline. Emails and other forms of online communication must be delivered to the intended recipient without the interference of the state or other third parties.[95]. Privacy is also related to the prohibition of discrimination (Article 2 ECHR), especially in cases including collection and use of big data within the aim of profiling and digital surveillance, even without suspicion of wrongdoing.[96]

[91] UN General Assembly, Report of the third Committee on the Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms, 8 December 2014, A/69/488/Add.2.

[92] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, A/HRC/23/40, p.7.

[93] UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Addendum, Communications to and from Governments, 16 May 2011, A/HRC/17/27.

[94] The Panopticon of Jeremy Bentham in: University College London, Bentham Project. See also: Reiman, J. (2004). Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posted by the Information Technology of the Future. In Privacies: Philosophical Evaluations, Stanford, Stanford University Press.

[95] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, A/HRC/23/40, p.7.

[96] UN Human Rights Committee (HRC), Concluding observations on the fourth periodic report of the United States of America, 23 April 2014, CCPR/C/USA/CO/4, p.3.

Copyright © Cyber-Trust Consortium. All rights reserved.

3. The concepts of privacy, security and surveillance in cyberspace

3.1 Privacy, cybercrime and cybersecurity

Cyberspace is continuously under attack. Cyber attacks happen every second, hampering the security of a network or a device. As cyberattack, in simple words, can qualify an attack launched from one device or more devices against another device, multiple devices or networks. The goal of those launching the attack, usually, is to disable the targeted device or put it offline. Other times, the primary goal is to get access to data stored in the specific device or perhaps gain admin privileges. Cyber attacks may vary in type and size. Attacks can range from planting malware which is downloaded to a targeted device and can be programmed to do anything from steal data to encrypt files and demand ransom, also known as ransomware to phishing emails that deceive victims into revealing passwords. Denial of Service attacks (DoS) may overwhelm a web server with traffic, and they can be distributed or not; Man-in-the-middle attacks aim to fool the target device into joining a compromised network. Wannacry and NotPetya ransomwares are only two examples of the most recent widespread cyber attacks, affecting thousands worldwide, including government services, companies and individuals.

Why are privacy and cybersecurity so closely connected? Perhaps because without some degree of privacy in the way they use their devices, people do not generally feel secure, and unless security is ensured, privacy is but an illusion. In cybersecurity, as perceived in the Cyber-Trust project, the notion of privacy that fits best is the informational one, but as seen above the privacy of communications may also play a role, depending on the specific tools used for the detection and mitigation of cyberthreats. Control over one's data can only be assured if the security of the data (confidentiality, integrity, and availability) is assured, otherwise the control is not real.

Concerns about security and privacy in the context of information processed by computers are nearly as old as the computing profession itself: the desire to break cryptographic codes triggered some of the earliest developments of digital computers.[97] With computers being built into sensors and control systems and with society's dependence on them continually growing, exploitation of security flaws has often resulted into deVere damage.[98] Aiming to build systems with as few security flaws as possible, requires developments in computing technology. Since the security of a device is often seen as an option and not an obligation, and frequently is addressed as an engineering cost that may even impede system functions, the economics of privacy and cybersecurity are a crucial factor in determining deployment of those technologies. However, it should be kept in mind that without neither a specified security policy nor a privacy policy, systems are vulnerable to attacks and in risk of severe legal violations.[99]

3.2 Privacy and digital surveillance in the context of cyber-threat intelligence gathering and attack detection

Privacy is also linked to the idea of surveillance. This is particularly true when privacy is related to the broad concept of "being left alone" or not "being steered" and not just a narrow one, i.e. relating to "informational privacy (see section 2.2.1). Surveillance may be considered intrusive by individuals even though the information that is collected is already in the public domain. This is because that even when cybersecurity measures do not need to use private personal information, they are still capable of extorting psychological pressure upon the individuals.[100] Looking at such matters in terms of purely informational privacy would not be sufficient to understand the harms that unnecessary surveillance can bring about.[101]

In the wake of advanced uses of information technology, it is necessary to view the "new surveillance"[102] or so-called, digital surveillance, as going beyond a simple vision of privacy as a form of informational control,

[97] C. Landwehr et al. (2012), Privacy and Cybersecurity: The Next 100 Years, in Proceedings of the IEEE, vol. 100, no. Special Centennial Issue, pp. 1659-1673.
[98] Ibid.
[99] Ibid.
[100] Nissenbaum, H. (1997).
[101] Marx, G.T. (1998), An Ethics For The New Surveillance**,** The Information Society, 14 (3).
[102] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

as described by *Nissenbaum.*[103] From an ethical point of view, the impact of surveillance can be assessed once the reasons for it have been defined.[104] Security often seems an easy answer to a possible why question, especially if it concerns surveillance in the form of filtering and monitoring for the prevention of crime or terrorist attacks, or in the form of security of network and information systems providing critical infrastructures, such as water or electricity. Once security is the response, the question that follows is whether security or this degree of security is justified under the specific circumstances and consequently, who is carrying out the digital surveillance and who is being monitored.[105]

In deciding upon whether a potential use would be acceptable, it would be necessary to take all such factors into consideration. Consequentialist approaches would justify large-scale digital surveillance in terms of achieving a greater good by taking into account the overall costs and benefits to the society, for instance, if the security of a community is best served by monitoring some or all the citizens. A deontological approach will find digital surveillance less acceptable if it interferes with certain rights of individuals such as the right to privacy because the theory looks rather to each entity monitored and its self-value than to the community as a whole. The type or tools of digital surveillance to be chosen in each specific case might also be influenced by whether a consequentialist or deontological justification is applied.[106]

The existence of a regime in which every digital interaction of every citizen, is collected and stored for real-time or future intelligence and law enforcement purposes may chill human relations and greatly affect the private sphere and family life of individuals.[107] "Those data [referring to metadata], taken as a whole, may allow precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."[108] The importance of fighting crime and protecting national security with the use of such pro-active techniques is not denied, however, as seen both in the case law of ECtHR and CJEU, a strict proportionality framework should be established (See sections 3.3.2 and 3.4.2.1), requiring that any interference with the broad notion of privacy be strictly necessary for the desired goal.[109]

A recognition of the harms that digital surveillance practices can produce for privacy in the broad sense, is vital in the context of the Cyber-Trust project, since the expected use of the Cyber-Trust prototype may involve monitoring of communications in public fora in the darknet and the clearnet as well as the use of publicly available blacklisted IP addresses and deep packet inspection techniques leading to the profiling of specific IoT devices for cyber-threat intelligence and attack detection and mitigation purposes. This is because individuals may not want to be monitored, even if in a public forum, or even if personal information that can be explicitly linked to them as individuals is not recorded. Individuals may, for example, feel disturbed at the prospect that the police could be alerted to their actions, even if they are not engaged in illegal activity.[110] The possibility of being monitored may induce people to behave differently or even avoid using apps, devices and services they regularly used before as part of their daily routine, having an effect on their personal autonomy. In this sense, the existence of digital surveillance systems should be considered from the perspective of privacy, even where they do not strictly pose a threat to individual privacy in the narrower "informational sense".

[103] Nissenbaum, H. (1997).
[104] Macnish, K. Surveillance Ethics, Internet Encyclopedia of Philosophy, iep.utm.edu
[105] Marx, G.T. (1998).
[106] Macnish, K.
[107] Fabbrini, F. (2015), Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S, in: Harvard Human Rights Journal 28, Tilburg Law School Research Paper No. 15/2014.
[108] CJEU, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Judgment of the Court (Grand Chamber), Joined Cases C-293/12 and C-594/12, 8 April 2014.
[109] Fabbrini, F. (2015).
[110] Nissenbaum, H. (1997).

Copyright © Cyber-Trust Consortium. All rights reserved.

3.3 Balancing competing values

3.3.1 A right to privacy cannot be (and is not) absolute

States and societies have many duties with regards to their citizens and residents. Whilst the protection of privacy is important; it represents but one of the duties states should try to fulfil.[111] Privacy is only one of the values that must be considered by a state. Other values are the security and the need for public order. If an any of those values were to be given an absolutist weight, the result would be a non-functioning society.[112] In order to assure security, the state will likely have to adopt measures that may interfere with the privacy of individuals. The state security structure may have to collect data or conduct acts of digital surveillance to prevent terrorism, for example. Individuals may have to restrain certain behaviours that they may have otherwise wanted to have engaged in.[113] As a result, the state often is called to strike a balance in order to uphold the rights of all groups in society to the greatest extent.[114] Various thinkers have considered this issue, and many have come to the conclusion that it is necessary to interfere with individual prerogatives only where there is a good reason to do so, and specific balancing exercises and safeguards are in place.[115]

3.3.2 The proportional nature of interferences with privacy

Whilst it may be apparent to most individuals that the state will sometimes have to interfere with the rights of some in order to protect those of others, the question remains as to how it should make such a decision on a case-by-case basis. One concept that is often given prominence in both ethical and legal thought is the notion of "proportionality".[116] Proportionality relates to the idea that the rights of some may be infringed if, in doing so, the aim is to minimise or avoid the harm that would be caused if the infringement had occurred.[117] Such an idea which the proportionality test, as seen later in section 3.3.2.1 is based upon, can help assess where certain actions are necessary or not. For most societies, the idea that the harms in terms of personal autonomy are less than the harm that would be caused by not mitigating a cyber attack or not prosecuting the criminals behind it is self-apparent. The notion of proportionality can often be applied to security measures that may interfere with personal privacy, since in specific instances, the measures in question may be proportional.[118]

For example, perhaps the Cyber-Trust prototype could be used to prevent or mitigate large-scale cyber attacks which could pose a serious danger for the smooth and safe operation of critical infrastructure. In such a case harms to personal privacy that might be experienced by some individuals due to the use of cyberthreat intelligence acquisition and sharing techniques are insufficient to render the aims behind the security measures, disproportionate.[119] In such instances was the state not to act in order to protect the critical infrastructure and consequently, human life would arguably not be meeting its obligations towards its citizens of providing security and protecting life and property. On the other hand, some security measures may be of questionable nature and disproportionate given the seriousness of the harms to privacy that are likely to occur, for instance when grave violations of privacy for the prevention or mitigation of minor threats to security or petty criminality occur.

One crucial aspect of the proportionality approach towards conflicting rights and interests is that it demands that there must be a justification for the state to interfere with the rights or interests of an individual or group

[111] Besson, S. (2015), The bearers of human rights´ duties and responsibilities for human rights: a quiet (r)evolution? Social Philosophy and Policy, 32(1), 244-268.

[112] Quinn, P. (2016).

[113] Brants, C. & Franken, S., (2009). The protection of fundamental human rights in criminal process General report. Utrecht Law Review. 5(2), pp.7–65.

[114] Besson, S. (2015).

[115] Brants, C. & Franken, S., (2009).

[116] Friedewald, M. J. [ed.] et al. (2017), Surveillance, Privacy and Security Citizens' perspectives, in New Security Studies, p.158.

[117] de Hert, P. and Gutwirth, S. (2009), Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalization in Action, in: Gutwirth, S., Poullet, Y., de Hert, P., de Terwangne, C., Nouwt, S. (Eds.), Reinventing Data Protection, Springer Netherlands.

[118] Ibid.

[119] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

in society.[120] Where such a reason does not exist, acting in a way that harms the rights or freedoms of some, including their privacy, will not be acceptable. The need to balance the competing values of privacy and security in society means that security measures that interfere with individual privacy are not acceptable unless they are intended to meet a need that is related to protection of the rights and interests of others.
Therefore, proportionality goes hand in hand with necessity. According to *Lango* two criteria are in place for measuring necessity:[121] the feasibility standard and the awfulness standard. The first occurs when there is enough proof to support that there is no feasible alternative, the second when the existing alternatives are worse than the proposed course of action. Whenever one of those criteria is met, the action may be deemed necessary. Proportionality in a broad sense embraces the necessity and the appropriateness of a measure, the "logical link" between the measure and the aim pursued.[122] Necessity, on the other hand, implies a fact-based assessment of the selective measure regarding its effectiveness for the objective pursued and of its intrusiveness compared to other available options for achieving the same goal.[123]
Given the harms of digital surveillance, it should, therefore, be avoided if there are in place other less harmful alternatives. If no alternatives are present, or when the alternatives would be more harmful, then surveillance may be justified. It is remarked that, according to the case law of the CJEU, an interference with the right to privacy in case of digital surveillance, can be established irrespective of whether the information concerned is sensitive or the persons concerned have been inconvenienced in any way.[124]

3.4 Legal approach to privacy

The notion of privacy is present in societies as such, as early as 1361 when the English Justices of the Peace Act provided for the arrest of peeping toms and eavesdroppers.[125] However, privacy was first conceptualized and protected in the ancient Greek and Chinese culture, as a right to solitude. Nowadays, over 130 countries worldwide protect privacy at constitutional level.[126] In other countries, where privacy is not explicitly recognized as a separate right in the constitution, such as in U.S.A., Ireland and India, the national courts have affirmed the protection of privacy based on other provisions.[127] Concerning the human rights treaties, the right to privacy has been more precisely interpreted in the context of the Art.17 ICCPR and the Art.8 of the ECHR, thanks to the case law that was developed around them.[128]

This section follows on from the discussion of privacy in its ethical dimension, by illustrating how the law recognises rights to privacy in the broad sense. This will first involve highlighting prominent sources of privacy rights in international and European law with a focus first, on the International Covenant on Civil and Political Rights and second, on the European Convention of Human Rights given its widespread application and binding nature for almost all states in Europe. The focus will be shifted to the applications of such legal principles to potential instances of digital surveillance and monitoring in the context of security, public order and prevention of crime. At the end of this section, these concepts will be discussed in the light of the Cyber-Trust project with the intention of highlighting the fundamental principles that should be born in mind throughout the project and in the data protection impact assessment which will be conducted in a next deliverable.

[120] Ibid.
[121] Lango, J. (2006), Last Resort and Coercive Threats: Relating a Just War Principle to a Military Practice. Joint Services Conference on Professional Ethics.
[122] European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017, p.5.
[123] Ibid.
[124] Ibid.
[125] Banisar, D. and Davies, S. (1999), p.9.
[126] Privacy International, "Victory! UK Surveillance Tribunal Finds GCHQ-NSA Intelligence Sharing Unlawful", (available at: https://www.privacyinternational.org/?q=node/485 [accessed July 24, 2015]).
[127] Banisar, D. and Davies, S. (1999), p.4.
[128] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

3.4.1 Prominent protection for privacy in international treaties

In international human rights law, privacy has always been regarded as a fundamental right and one of the foundations for a democratic society.[129] The right to privacy can be found in all of the primary international and regional human rights instruments, including: United Nations Declaration of Human Rights (UDHR) 1948, Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Whilst this is non-binding on the legal systems of individual states, it is nonetheless of considerable symbolic importance. It is worthy to mention that during the drafting of UDHR, the staff working on the right to privacy used the language of inviolability. Such strong language is used only for very special types of rights.[130] Nevertheless, in the end, the phrase was dropped since very soon came the realization that the right to privacy is not an absolute one, as it was discussed in Section 3.3.1.

The right to privacy is also protected in the International Covenant on Civil and Political Rights (ICCPR) 1966, Article 17: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation. 2. Everyone has the right to the protection of the law against such interference or attacks." The ICCPR signatory states are themselves bound to uphold the standards enhanced in the Covenant. Nevertheless, in contrast with other human rights instruments, such as ECHR, which provide for a proper judicial body committed to enforcing their provisions, the ICCPR is limited to a monitoring and complaints-handling committee, the Human Rights Committee, where individuals can launch complaints upon exhaustion of domestic remedies, given that the state party concerned has signed and ratified the first Optional Protocol to the Covenant.[131] The views of the Committee concerning the complaints are not binding under international law, but they carry a special weight. So do its reports and views on relevant matters.

The Human Rights Committee (HRC) in its case law recognizes that the right to privacy covers further rights. In *Coeriel and Aurik v. The Netherlands*, the Committee observes that the right to privacy also protects the right to express one's identity freely.[132] In *Leo Hertzberg et al. v. Finland*, three members of the Committee observed that Article 17 encompasses "the right to be different and live accordingly."[133] Last but not least, the Committee in its General Comment no.16, supports that the right to privacy also encompasses another right, that is intimacy.[134]

The discussion in literature and case law is also reflected in the effort to interpret the term "privacy", as provided in Art. 17 ICCPR. Although its meaning has not been authoritatively clarified in the General Comments of the Human Rights Committee or its relevant case-law,[135] privacy in legalese has been generally understood as the right to be left in solitude, and in a more concrete sense as the right to have control upon one's own information.[136] [137] Art. 17 ICCPR also holds guarantees for a right of intimacy, in terms of secrecy of private behaviour, including keeping actions or personal data secret from the public sphere. Furthermore, it seems to be similar to the provision of Art.8 of the European Convention of Human Rights (ECHR), despite their different wording, by taking into account that practitioners and scholars, when dealing with the normative substance of Art. 17 ICCPR, often refer to the findings of the European Court of Human Rights

[129] Electronic Frontier Foundation and Article 19 (2014), Necessary and proportionate: International Principles on the Application of Human Rights Law to Communications Surveillance, Background and Supporting International Legal Analysis, available at: http://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf, p.14.

[130] Johannes Morsink, (2000) The Universal Declaration of Human Rights: Origins, Drafting and Intent, Pennsylvania Studies in Human Rights: Philadelphia: Univ. of Pennsylvania Press.

[131] UN General Assembly, Optional Protocol to the International Covenant on Civil and Political Rights, 19 December 1966, United Nations, Treaty Series, vol. 999, p. 171.

[132] Coeriel et al. v. The Netherlands, Communication No. 453/1991, U.N. Doc. CCPR/C/52/D/453/1991 (1994).

[133] Leo Hertzberg et al. v. Finland, Communication No. 61/1979, U.N. Doc. CCPR/C/OP/1 at 124 (1985).

[134] UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988.

[135] Joseph, J., Schultz, S. J. and Castan, M. (2004), p.477.

[136] Warren, S. D. and Brandeis, L.D. (1980), pp.193, 195.

[137] Westin, A. F. (1967). See also: Fried, C. (1968), Privacy, in: Yale Law Journal Vol.77, p.483.

Copyright © Cyber-Trust Consortium. All rights reserved.

(ECtHR).[138] *Mutatis mutandis*, the European Convention on Human Rights (ECHR) in many circumstances reflects the principles and ideas encompassed in the ICCPR since its drafting was based on an early draft of the Covenant.[139]

3.4.2 Privacy at the European Level

The European Union's Charter of the Fundamental Rights (CFR) which entered into force after the enactment of the Lisbon Treaty explicitly recognizes a fundamental right to privacy in Article 7 under the notion "respect for private and family life", stating: "Everyone has the right to respect for his or her private and family life, home and communications." The scope of this Article is however restricted to the activities of European Institutions and the implementation of EU law. The application in the field of criminal law is thus likely to be limited given that the EU's competence on laws relating to national criminal justice related practices is respectively limited.

The European Convention on Human Rights (ECHR), given its widespread application worldwide as well as in the EU Member States, seems to be of more relevance. Furthermore, the rulings of the European Court of Human Rights (ECtHR) are binding upon the legal systems of the Member States,[140] having the power to give rise not only to the possibility for damages or other reparations for individual complainants but also setting precedents for future interpretation of national law.

Article 8 of the ECHR

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

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

3.4.2.1 Security, surveillance and privacy in the ECtHR case law

Article 8 ECHR has been interpreted by the court in several cases related to both the narrow "informational" concept of privacy as well as in cases in the broader privacy sense. It becomes obvious that the right to respect for private life is granted to all individuals within the jurisdiction of a State Party, regardless of their nationality or place of residence. The ECtHR in *Botta v. Italy* found that concerning Article 8 of ECHR, "private life" includes a person's physical and psychological integrity as well as the development of their personality, without outside interference.[141] In *Peck v. the United Kingdom*, the Court identified a "right to identity and personal development" as well as a right to establish relationships with human beings and the outside world.[142]

With regards to surveillance systems, the ECtHR has, for example, stated that:[143] "There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. […] Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security

[138] Georgieva, I. (2015), The Right to Privacy under fire – Foreign surveillance under the NSA and the GCHQ and its compatibility with Art. 17 ICCPR and Art. 8 ECHR, in: Utrecht Journal of International and European Law, Vol.31(80).

[139] McCrudden, C., Human Dignity and Judicial Interpretation of Human Rights, in: European Journal of International Law Vol.19(4) (September 1, 2008), pp. 655–724.

[140] Abdelgawad, E.L. (2009), The Execution of the Judgments of the European Court of Human Rights: Towards a Non-coercive and Participatory Model of Accountability, ZaöRV 69 (2009), 471-506.

[141] Botta v Italy, App. no. 21439/9, ECtHR, judgment on merits, Reports 1998-I, 24 February 1998.

[142] Judgment by the European Court of Human Rights (Fourth Section), case of Peck v. United Kingdom, Application no. 44647/98 of 28 January 2003.

[143] Nash, S. (2002), Balancing Convention Rights: P.G. and J.H. v United Kingdom in: The International Journal of Evidence & Proof, Vol 6, Issue 2, pp. 125 – 129.

Copyright © Cyber-Trust Consortium. All rights reserved.

services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method."[144]

The Court, therefore, accepts that in general, surveillance systems in public places, including the internet, are capable of engaging individual rights under Article 8 ECHR. The concepts of "private life" and "correspondence" include telephony and telecommunications data.[145] The case law of the ECtHR specifies that the scope of protection of this fundamental right covers not only the content of communications but also "traffic data" or "metadata".[146] Not all "engagements" can automatically be equated to violations of Article 8. According to Article 8(2) ECHR, interference by a public authority with the exercise of the right to respect for private life may only be accepted if such restriction:

- is in accordance with the law, which must have foreseeable consequences and be generally accessible and;
- is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, or the protection of health or morals, or for the protection of the rights and freedoms of others.

Exceptions to rights guaranteed by the Convention are to be narrowly interpreted.[147] Thus, an interference may be necessary if it constitutes the response to a pressing social need, is proportionate to the aim pursued and if the reasons put forward by the public authority to justify it are relevant and sufficient.[148] In the EU context, the Court of Justice of the European Union (CJEU) has also stated that, for the interference to be proportionate, it has to be demonstrated that other less intrusive methods were not available or would not have the same desirable results.[149] In the case of national security, the ECtHR has noted that arrangements governing the foreseeability requirement may differ from those in other areas but that the law must at all events state under which circumstances and subject to what conditions the state may carry out secret, and thus potentially dangerous interference within the exercise of the right to respect for private life.[150] The nature of the points raised here indicates the contextual nature of the decision that must be made on particular surveillance practices on a case-by-case basis. When the interferences take place in a secret or another covert manner, due to the fact that the affected persons are unaware of the measyres and do not have the possibility to challenge it, very well-developed safeguards must be put in place in conjunction with very strict standards.[151]

In accordance with Article 8 ECHR, the European Court of Human Rights is entitled to take security into account as a legitimate interest in the sense of national security, public safety or the prevention of disorder or crime. The ECtHR case law seems to prioritise a proportionality test when discussing privacy and security. According to this test, courts have to choose between two or more conflicting rights and interests and set up a balance. The proportionality test includes four sub-tests.[152]

[144] See: Rotaru v. Romania [GC], no. 28341/95, §§ 43-44, ECHR 2000-V).

[145] Article 29 Working Party, Working Document on surveillance of electronic communications for intelligence and national security purposes, 5 December 2014, 14/EN WP 228, p.16.

[146] Loideain, N.N. (2015), EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era in: Media and Communication, 2015, Volume 3, Issue 2, pp. 53-62, p.55.

[147] See: ECtHR, Klass and others v. Germany, 6 September 1978, para. 42.. See also: Youth Initiative for Human Rights v. Serbia,2 5 June 2013, §§24-26, which confirms that also intelligence agencies have to comply with fundamental rights and national laws.

[148] S. and Marper v. United Kingdom, Applications nos. 30562/04 and 30566/04, Council of Europe: European Court of Human Rights, 4 December 2008. The Court specified that the blanket and indiscriminate retention of sensitive data of the applicants, as persons who had been suspected, but not convicted, was not justified under Article 8 § 2 of the Convention.

[149] See CJEU, Joined Cases C-92/09 and C- 93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, 9 November 2010, para. 81.

[150] Article 29 Working Party, Working Document on surveillance of electronic communications for intelligence and national security purposes, 5 December 2014, 14/EN WP 228, p.17.

[151] Council of Europe, Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, home and correspondence, updated on 31 August 2018, p.37.

[152] Friedewald, M. J. [ed.] et al. (2017), pp. 158-159.

Copyright © Cyber-Trust Consortium. All rights reserved.

During the first sub-test, a purpose can justify the limitation of a fundamental right if it is considered legitimate in a democratic society.[153] Protecting human rights and, to a certain extent, satisfying public interests - in this case, the public interest of security - can be seen as a legitimate aim in a democracy. The second sub-test is to determine whether the limitation of the fundamental right concerned – in case a legitimate aim was found in the first sub-test – is suitable for realising the aim pursued.[154] In the third sub-test, after having established the legitimacy of the aim and the suitability of the limitation, the necessity of the limitation is examined, in other words, whether the limitation applies the less restrictive means in order to achieve the legitimate aim.[155] The fourth and final sub-test, the proportionality test *in stricto sensu* requires balancing between the two values under examination: on the one hand, the aim of the limitation (for instance, preventing a cybercrime, therefore ensuring security) and, on the other hand, the limited fundamental right (the right to privacy).[156] The limitation of a fundamental right is justified only if a proper relation between the benefit gained and the harm caused is established after careful examination of all specific aspects.

For instance, in January 2016, the European Court of Human Rights (ECtHR) delivered a judgment in the case of *Szabo and Vissy v. Hungary.* The ECtHR concluded in its ruling that broad secret surveillance conducted by the Hungarian Anti-Terrorism Task Force, as part of the police force, on the basis of the 2011 anti-terrorism domestic legislation, had violated Article 8 ECHR on the following grounds:[157] the scope of the surveillance practices "could include virtually anyone"; the authorisation order was not issued by a judicial authority; no assessment of strict necessity took place; the vastness of data intercepted affected persons outside the scbe lawope of the operations, and; no mechanisms for effective judicial oversight were put in place.

By contrast, in a more recent judgment on *Centrum För Rättvisa v. Sweden on* 19 June 2018,[158] the Court held that legislation allowing the mass interception of electronic signals in Sweden for foreign intelligence purposes did not violate Article 8 ECHR. It held that despite a system of covert surveillance and monitoring that potentially indiscriminately affected all users of mobile telephones and the internet, without them being notified, overall the Swedish system of bulk interception provided sufficient guarantees against arbitrariness and the risk of misuse. In particular, the Court took into account whether the scope of the measures and the handling of intercepted data were defined in law; whether the measures were only permitted in a strictly specified area, i.e. communications crossing the Swedish border; the retention time of data, which was no longer than 6 months; whether the authorisation for interception was given by a court order; whether independent oversight and review mechanisms as well as complaint and notification mechanisms were in place.

The Court also considered the State's discretionary powers in protecting national security, especially given the threats of global terrorism and serious cross-border crime, following the logic also present in the judgment on the *Klass and others v. Germany*,[159] where it concluded that the existence of legislation that permits secret surveillance over the mail, post and telecommunications was, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime.

3.4.2.2 General privacy approaches – key points for the Cyber-Trust project

The proposed Cyber-Trust prototype represents a technology that will be used for cyberthreat intelligence gathering and sharing purposes, with the aim to contribute to information and network security, while eliminating the number of cyberthreats, by deploying detection and mitigation tools. As such, the Cyber-Trust prototype will use monitoring and filtering techniques in the context of intelligence gathering and

[153] Ibid.
[154] Ibid.
[155] Ibid.
[156] Ibid.
[157] ECtHR, Judgment (Merits and Just Satisfaction) of 12 October 2016, Szabo and Vissy v Hungary, appl. no. 37138/14, para 89.
[158] ECtHR, judgment of 19 June 2018, Centrum För Rättvisa v Sweden, appl. no. 35252/08.
[159] Klass and others v Federal Republic of Germany, European Court of Human Rights (Series A, NO 28) (1979-80) 2 EHRR 214, 6 September 1978.

Copyright © Cyber-Trust Consortium. All rights reserved.

attack detection, which could amount to digital surveillance with the potential to affect the privacy of individuals. Such intrusions in privacy could occur whenever digital surveillance takes place in the public sphere, "secluded" public areas or "closed" spaces online (though the privacy intrusion would be of a much graver nature in the last case). However, such intrusions in privacy may not necessarily constitute privacy violations, since the context in question should be taken into consideration.

Article 8 ECHR recognises that measures may be necessary and proportional to address crime and establish public order, by offering a qualification to its general protection *inter alia* for crime-preventive measures. As discussed earlier, this does not mean that the mere fact that where a Cyber-Trust prototype is used in order to detect or prevent crime, its use will automatically be legal. This is because the use of such a tool in a particular context would have to meet the conditions of proportionality and necessity, as well as to take into account and comply with the specific national law in each case since police and justice matters are regulated by the domestic law of the Member States.[160]

The competing notions of privacy and security are obviously relevant in the context of the Cyber-Trust project, because by its very nature, it poses a risk to privacy, whether this be in the narrow informational sense or the broader sense. Thus, it is important to discern if, where and how Cyber-Trust will make use of information that could lead to the identification of an individual. Wherever it does, it would be necessary to comply with the relevant data protection frameworks, as described in Part B. It is important however to recognize that privacy does not only relate to information concerning a specific individual but can also be thought of on a broader sense.

Such potential interferences with personal privacy are not always unacceptable. For instance, potential uses in incidences relating to cybercrime and cybersecurity for which Cyber-Trust is intended, depending on the level of intrusion of privacy that occurs, may be acceptable in specific contexts. The concept of proportionality provides a way of judging when such interferences may be acceptable. In terms of possible interference with privacy, imagine the difference between an interception system that scrapes all the available data on an internet platform and a digital surveillance system that is only activated by certain incidents that are more likely to correlate to criminal activity. Imagine also the aim of the measures in question. Are they intended to tackle serious crime (e.g. cyber-attacks on critical infrastructure) or are they intended to tackle petty criminality, as well (small scale cyberthreats with minor or uncertain impact)?

On that note, Cyber-Trust as a research project is able to make a difference to the question of proportionality, and therefore legality, by making the design of the tool in question as "privacy-friendly" as possible. Doing so, for instance by designing the tool in a way that is able to detect and record activity that is highly likely to be of criminal nature, the chances are higher that the use of the tool in a particular circumstance will be deemed as being proportional. Police, prosecutors and investigative judges will consider the proportionality question when deciding upon requests to deploy the tool. Moreover, a failure to engage privacy enhancement tools could have as a result that the Cyber-Trust prototype is used only in the gravest of contexts and would reduce both its appeal and potential uptake by end-users, which are not competent authorities or law enforcement agencies.

For instance, when designing the web crawler, [161] it is crucial for the Cyber-Trust partners to keep in mind that the usage of such a prototype by its end-users should demonstrate compliance with the notions of data protection by design and by default by a) conducting prior data protection impact assessments, b) having policies in place that clarify the legal grounds for using the tool, in cooperation with their Data Protection Officers, wherever necessary and c) having internal and external oversight mechanisms, including in seeking appropriate authorisations.[162] This means that the crawler that is intended to be used in Cyber-Trust is recommended to be coded in a manner that would reduce the possibility for unintentional problems on websites.[163] Similar thoughts will be addressed in section 7.3, relevant to the use of Blockchain technologies for the storage of electronic evidence and other special issues.

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

[161] Zouave, E. (2017), Law Enforcement Webcrawling: Lawfulness by Design and by Default, DANTE project, KU Leuven CiTiP.

[162] Ibid.

[163] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

Part B – Data Protection

4. Data Protection – The European Legal Framework applicable to Cyber-Trust

Section 4 will explore the potential impact of European data protection law on the Cyber-Trust project, with emphasis on the EU law and the law by the Council of Europe (CoE). Since in the context of Cyber-Trust, there is a possibility that personal data may be processed, data protection law will be most relevant with respect to cyber-threat intelligence gathering and sharing, attack detection and mitigation techniques, as well as IoT device profiling and storage of evidence in blockchain, for example, if the conducted research involves individuals that can be identified.

The right to respect for private life and the right to personal data protection are closely related, but distinct; closely related, because both are set to protect the autonomy as well as the human dignity of individuals and constitute a prerequisite for the exercise of other fundamental freedoms, such as the freedom of expression; distinct, because data protection is conceptually different from the privacy approach.[164] The difference is detected both in their formulation and in their scope. The right to privacy can be seen as a general prohibition on interference, subject to some public interest constraints, whilst personal protection is considered a modern legal norm, ensuring an active right, building upon a set of balancing checks, rules and principles that must be adhered to in all cases of data processing.[165] The right to privacy presupposes that a private interest, or more specifically the private life of the individual has been compromised, and the relevant assessment depending on the particular facts and contexts of each case does not justify any such interference. To the contrary, any operation involving the processing of personal data of all kinds could fall under the scope of data protection rules, irrespective of the impact of such operation on privacy, as already discussed in session 2.2.2.

The personal data protection approach is structured upon two pillars: the processing must comply a. with the independent supervision requirement and b. with respect for the data subject´s rights. In each EU Member State, compliance with the right to data protection is subject to control by an independent authority.[166] Failure to comply with the laid rules and principles could give rise to legal action against the data controller – as described next - and the possibility of damages for the affected data subjects.

4.1.1 Definition of personal data

Under EU law as well as under CoE law, information contains personal data, if:

- an individual[167] is identified or identifiable by this information; or
- an individual, while not identified can be singled out by this information in a way which makes it possible to find out who this individual is by conducting further research.

Personal data include any kind of information, related both to matters of the private - including professional sphere - and public life of the individual. Both direct and indirect identifiability require continuous assessment.[168] The Recital 26 of the GDPR introduces a case-by-case approach and reads: [to] “ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the cost of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments”. Identifiability is understood in a similar way under CoE law.[169]

In accordance with both the EU and CoE law, "data processing" means any operation performed on personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval,

[164] European Union Agency for Fundamental Rights (FRA) and Council of Europe (CoE), Handbook on European Data Protection Law, 2018 edition, p.18. (hereinafter, Handbook on European Data Protection Law (2018)).
[165] de Hert, P. and Gutwirth, S. (2009).
[166] Handbook on European Data Protection Law (2018).
[167] Or, a “data subject”.
[168] Handbook on European Data Protection Law (2018).
[169] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (plus, preservation in the Convention 108+). Data about a deceased person or information about legal entities or public authorities is not personal data.[170] The Directive 2016/680 highlights the distinction among different categories of data subjects (suspects, convicted persons, victims, witnesses), as something that has to be taken into consideration by the national legislator.[171]

An individual is "identified" or "identifiable" if you can distinguish them from other individuals. For instance, a name is usually used for identification purposes. However, the specific context would always determine whether any potential identifier leads to the identification of an individual. Often a combination of identifiers might be needed to identify an individual. The GDPR provides a non-exhaustive list of identifiers, including: a. name; b. identification number; c. location data; and d. an online identifier.

4.2 The Council of Europe's data protection approach

In 1950, the CoE adopted the European Convention on Human Rights (ECHR), which entered into force in 1953. The right to data protection is indirectly part of the non-absolute rights enshrined in Article 8 of the ECHR, namely the right to respect one´s private and family life, home and correspondence, which in turn, correspond to both positive and negative obligations of the Contracting Parties. To ensure that the Parties observe those obligations, the European Court of Human Rights (ECtHR) was established in 1959. Since then, the ECtHR has examined and decided upon many cases involving data protection issues.

The Convention for the protection of individuals with regards to the automatic processing of personal data (Convention 108) was opened for signature in 1981. The Convention applies to both the private and the public sector (Article 3(1)), including judiciary and law enforcement matters, unless a member state opt-outs (Article 3(2)). As of 2018, 51 countries are parties to Convention 108, which remains the only legally binding international document in the data protection field. All EU Member States have ratified the Convention 108, which recently underwent a significant modernisation process (Convention 108+) and was completed with the adoption of the Protocol CETS No. 223.[172] Over the years, several non-legally binding recommendations (e.g. the Police Recommendation) have been adopted by the CoE´s Committee of Ministers. Although Convention 108 is not subject to the judicial supervision of the ECtHR, the principles enshrined in it have been repeatedly taken into consideration in its case law. The modernisation process of the Convention 108, carried out in parallel with the EU data protection legislative reform, aimed to ensure consistency between the two legal frameworks.[173]

4.3 The European Union's data protection approach

The EU's data protection approach has created law that is binding in all Member States of the EU. The principles and rules it introduces are capable of giving rise to both legally enforceable obligations for data controllers/processors, and rights for the data subjects concerned. EU rules concerning data protection are found both in primary law in the form of general principles and commitments that often comprise the legal basis for more precise legislative and judicial initiatives, and in secondary law, in the form of more elaborate binding rules applicable in a wide range of situations.

4.3.1 Fundamental commitments in primary law

The entry into force of the Lisbon Treaty in 2009, amending the Treaty of the European Union (hereinafter, TEU) and the Treaty of the Functioning of the European Union (hereinafter, TFEU), is a milestone for the development of the data protection law in EU for two reasons.[174] On the one hand, the Lisbon Treaty elevated the 2000 Charter of the Fundamental Rights of the European Union (CFR) at the level of primary law, making

[170] Ibid.
[171] Article 4 Directive 2016/680.
[172] 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.
[173] Handbook on European data protection law (2018).
[174] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

its provisions binding for the EU institutions and bodies as well as for the Member States, whenever they implement EU law (Article 51 CFR). The Charter provides for two separate fundamental rights, the right to private and family life (Article 7 CFR) and the right to the protection of personal data (Article 8 CFR), as it reads below:

Article 8 CFR

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

On the other hand, the Lisbon Treaty provided for the right to the protection of personal data. Article 16 of the TFEU introduces the right explicitly and creates a new independent legal basis, for the adoption of comprehensive EU data protection legislation.[175] Article 39 of the TEU also refers to the processing of personal data by the Member States.

4.3.2 Data protection in secondary law

Legal declarations such as those above represent general requirements and principles that apply in the interpretation and application of European Union law. Of more practical importance are the specific legislative initiatives that EU has taken with regard to data protection. From 1995 until May 2018, the principal EU legal instrument was the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data (Data Protection Directive).[176] Until recently, these initiatives have generally taken the form of Directives which have been transposed into national law, giving space for some variation along national lines. However, with the adoption of the General Data Protection Regulation (GDPR), this approach is being overtaken by an effort to harmonise Member States law with the adoption of appropriate Regulations. The most important of these legislative initiatives are:

4.3.2.1 Regulation 2016/679 (General Data Protection Regulation)

The full name of this legislation is Regulation 2016/679 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. It is otherwise known as the General Data Protection Regulation and replaces the previous regime of European data protection law embodied in Directive 95/46/EC. As a Regulation, it takes force in the Member States directly. Nevertheless, Member States can opt for derogations with regard to specific provisions. The GDPR primarily addresses Article 8 of the CFR.[177]

4.3.2.2 Directive 2016/680 (Police and Criminal Justice Data Protection Directive)

Part of the EU data protection reform package along with the GDPR, the full name of this legislation is 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.[178] It aims to protect individuals' personal data when the latter is being processed by police

[175] Ibid.

[176] European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995.

[177] Handbook on European Data Protection law (2018).

[178] 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.

Copyright © Cyber-Trust Consortium. All rights reserved.

and criminal justice authorities and improve the mechanisms of cooperation in the fight against terrorism and cross-border crime in the EU.[179]

Cross-border cooperation particularly in combatting cross-border crime is also regulated by the Prüm Decision (Council Decision 2008/615/JHA)[180] and the Swedish Initiative (Framework Decision 2006/960/JHA)[181]. Member States were invited to adopt and publish, by 6 May 2018, the laws necessary to comply with this Directive, but the process is still ongoing.[182]

4.3.2.3 Directive on privacy and e-communications (e-Privacy Directive)

The full name of this legislation is Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.[183] The Regulatory Framework for Electronic Communications, which the e-Privacy Directive belongs to, applies to providers of electronic communications networks and services. More precisely, according to Art. 3, the Directive is applicable "to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community." Consequently, "only services consisting wholly or mainly in the conveyance of signals – as opposed to, e.g. the provision of content or other value-added services" are within the scope of the Directive.[184] The latter is not applicable to issues of law enforcement and criminal prosecution. It was adopted in 2002 and amended in 2006 and 2009.

Nevertheless, in January 2017, the Commission adopted a new proposal for an e-Privacy Regulation,[185] to replace the old Directive and enforce a unified approach across every Member State and type of data controller.[186] The proposed Regulation aims to address Article 7 of the CFR and would be *lex specialis* to the GDPR, tailoring data protection rules to electronic communications, including explicitly electronic communications content and metadata.[187] A brief look at the critical aspects of the proposed Regulation, as follows:[188] fines and sanctions would be in line with GDPR relevant provisions; also proposed to have extra-territorial effect; extends from traditional telecommunication service providers to: (i) "over the top" service providers; (ii) M2M communications (i.e. IoT technology), and (iii) probably all services with an electronic communications element; rules on direct marketing and use of cookies and other tracking technologies would apply to all marketers and websites, whereas do-not-track and anti-cookie wall policies would enter into force, requiring consent with few limited exceptions, for example for security updates or audience measurement on websites.[189]

---

[179] Handbook on European data protection law (2018).

[180] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 1–11.

[181] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p. 89–100.

[182] Handbook on European data protection law (2018).

[183] European Union, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2000/0189/COD.

[184] European Commission, DG Communications, Networks and Technology, ePrivacy directive, assessment of transposition, effectiveness and compatibility with the proposed data protection regulation, Digital Agenda for Europe, 2015.

[185] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD).

[186] Kuner, C. (2007), European Data Protection Law: Corporate Compliance and Regulation, Second Edition, OUP UK.

[187] Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, 28 May 2018.

[188] Ibid.

[189] Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, 28 May 2018.

Copyright © Cyber-Trust Consortium. All rights reserved.

4.3.2.4 Invalid Directive 2006/24/EC (Data Retention Directive)

Directive 2002/58/EC was amended by the Directive 2006/24/EC.[190] This latter directive, also referred to as Data Retention Directive, does not contain directly rules applicable to electronic evidence. Nevertheless, it obliged telecommunication service providers to store certain traffic data for a period of six to twenty-four months for the purpose of making them available on demand of prosecution authorities. However, in 2014 in the case of Digital Rights Ireland, the CJEU declared the Directive invalid *ex tunc* since it interfered with the fundamental rights to respect for private life and protection of personal data and exceeded the limits of the principle of proportionality as provided for in the Charter.[191] National legislations still need to be amended, however only regarding aspects that became contrary to EU law after the judgement. In other words, the fact that the Directive was declared invalid does not affect the ablility of the Member States under the e-Privacy Directive (2002/58/EC) to continue requesting retention of data.[192]

Some general observations with regards to case law in the matter are deemed necessary. In the case of *Tele2 Sverig*e and *Home Secretary v. Watson*[193], the court concluded that the Member States could not impose a general obligation on providers of electronic telecommunications services to retain data. Nevertheless, it did not proceed to ban data retention altogether either. Data retention is in compliance with EU law if it satisfies two specific conditions: a. it is deployed against specific targets to fight serious crime and b. the measures are necessary and proportionate with regards to the categories of data, the means of communication impacted, the persons concerned and the duration of retention.[194] Furthermore, state authorities can access the retained data only under certain conditions and data protection safeguards.[195]

In the case of *Breyer*[196]*,* the Court held that Internet Protocol addresses may constitute personal data if the individual concerned can be identified, even where a third party must obtain additional data first. The CJEU also concluded that data retention is allowed based on the legitimate interest of the website operators for retaining and using their visitors' personal data.[197] This decision is of major significance since it entails that online media service providers may lawfully store their visitors' personal data to pursue a legitimate interest, rather than just for the purposes previously outlined in the invalid Data Retention Directive, broadening this way the grounds justifying data retention.[198]

Member States seem to be reluctant adopting new legislation for data retention, taking into account the requirements and safeguards that the CJEU's case law has laid out. However, a brief overview of the current state of the relevant legislation in the Member States of interest for the partners follows below.

i. Cyprus

Although the Directive was invalidated by CJEU, the Law 183(I)/2007 which transposed it in the domestic legislation is still valid. The national law is rooted from the constitution and includes specific safeguards for the protection of privacy; for example, communication data are released only following a court order. In 2014 a case was filed with the country´s Supreme Court attempting to use the CJEU ruling to overturn convictions in cases where critical evidence was collected via mass storage of personal data. However, the Supreme Court found that the law complied with the European Convention on Human Rights and that data retention is a

[190] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63.

[191] CJEU, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Judgment of the Court (Grand Chamber), Joined Cases C-293/12 and C-594/12, 8 April 2014.

[192] European Commission, Memo, Frequently Asked Questions: Data Retention, Brussels, 8 April 2014, available at: http://europa.eu/rapid/press-release_MEMO-14-269_en.htm [Accessed: 06.08.2018].

[193] CJEU, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, Judgment of the Court (Grand Chamber) of 21 December 2016, Joined Cases C-203/15 and C-698/15.

[194] FRA, Fundamental Rights Report 2017.

[195] Ibid.

[196] CJEU, Patrick Breyer v Bundesrepublik Deutschland, Judgment in Case C-582/14, Luxembourg, 19 October 2016.

[197] FRA, Fundamental Rights Report 2017.

[198] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

proportionate measure for combating crime.[199] The government, moreover, proposed draft legislation to the parliament that obliges telecom companies to register the users of prepaid cards.

ii. Greece

In Greece, Act 3917/2011 implemented Directive 2006/24/EC (Data Retention Directive), and notwithstanding the fact that CJEU invalidated the Data Retention Directive, it is still in force. The Ministry of Justice, however, has formed a Special Legislative Committee for the proposition of annulment or amendment of the national law in order to comply with the CJEU Judgment.[200] Albeit, at the moment, communications and Internet Service Providers are obliged according to Act 3917/2011, to retain the content of communications; retain the traffic and location data within the premises of the Greek territory for 12 months. The LEAs may access the data under the conditions and requirements of Act 2225/94 for national security reasons and for investigation or prosecution of particularly serious crimes, in the execution of a judicial order.

Except for Act 3917/2011, there is a number of other Laws and Acts, covering the issue of data retention. Act 2225/1994 provides the legal requirements and the judicial procedure for the lawful interception of the content of communications and access to communications data; Act 3115/2003 provides the legal framework relating to the constitution, the operation and the functions of the independent administrative authority A.D.A.E. monitoring the protection of confidentiality of communications, procedure of lawful interception and access to communications data and application of the Data Retention Directive; the Presidential Decree 47/2005 under the title "Procedure, technical and organisational guarantees for ensuring lawful interception" provides for the technical and organisational measures for lawful interception and access to data; Act 3471/2006 implemented Directive 2002/58/EC (e-Privacy Directive), while Act 3674/2008 refers to the security of the Provider's services and their obligations; Act 3783/2009 refers to the traceability of mobile phone users and ban of anonymity of prepaid SIM card-users; Act 4070/2012 amended the aforementioned Act 3471/2006, implemented Directives 2002/19/EC, 2002/20/EC, 2002/21/EC, 2002/22/EC and 2002/77/EC as amended by the Directives 2009/136/EC and 2009/140/EC and provided the legal framework for the constitution, operation and functioning of the National Regulatory Authority "Hellenic Telecommunications and Post Commission".

iii. Italy

See section 5.3.2, concerning the transposition of the Directive 2016/680 in the national law.

iv. Luxembourg

In Luxembourg, the government introduced Bill No. 6763 in 2015, which amends the data retention rules in line with the case of Digital Rights Ireland and limits the possibilities of data retention to the grounds listed explicitly in the bill, restricting the retention period to 6 months.[201]

v. The Netherlands

Under the Dutch law implementing the Data Retention Directive, telephone companies were required to store information about all phone calls for one year, whilst Internet Service Providers had to store information on their clients' internet use for six months. The Telecommunications Data (Retention Obligation) Act was declared inoperative in 2015. The court was of the opinion that under the Act, the violation of privacy was not limited to what is strictly necessary, and the judgment concluded that scrapping

[199] Cyprus / Supreme Court / Joint cases 216/14 and 36/2015, available at: http://fra.europa.eu/en/caselaw-reference/cyprus-supreme-court-joint-cases-21614-and-362015 [Accessed: 05.08.2018].

[200] The information available in English was taken from: http://www.greeklawdigest.gr/component/k2/item/84-privacy-data-retention-and-data-protection-in-the-electronic-communications-sector-providers-of-publicly-available-electronic-communications-services-competent-supervisory-independent-administrative-authorities [Accessed: 09.08.2018].

[201] FRA, Fundamental Rights Report 2017.

Copyright © Cyber-Trust Consortium. All rights reserved.

the data storage "could have far-reaching consequences for investigating and prosecuting crimes".[202] Based on that decision, providers in the Netherlands are no longer obliged to retain data for criminal proceedings. Law enforcement agencies can still request data after the annulment, but without the retention requirement, the results of any such application are entirely dependent upon the provider, who can decide what information to keep, and for how long.

Nevertheless, the Dutch Public Prosecution Service expressed their concerns over this development and its likely repercussions for detecting cybercrimes and other offences.[203] Since, in practice, in the case of internet-related crimes, it is quite common for a suspect not to be identified right after, investigators consider it essential that certain "old" data remain available to assist them in their inquiries.[204] The Dutch Council for the Judiciary too, in a legislative recommendation issued in February 2015, stressed the importance of such a requirement whilst at the same time acknowledged the need to protect individuals' fundamental rights. It, therefore, proposed a system whereby requesting the disclosure of telecommunications traffic data would require an order by an investigative judge.

The Dutch Ministry of Justice is planning to introduce new legislation on the matter, after unsuccessful several attempts to adopt data retention laws anew.[205]

vi. United Kingdom

The Investigatory Powers Acts provide for the Secretary of State to require communication service providers to retain communications data for one or more of the statutory purposes. The Data Retention and Investigatory Powers Act 2014 was an Act of the Parliament of the United Kingdom that received Royal Assent on 17 July 2014 and allowed security authorities to continue having access to phone and internet records of individuals despite the CJEU invalidation ruling. In 2016 the CJEU ruled in joined cases that the Data Retention and Investigatory Powers Act 2014 was unlawful.[206] The Data Retention and Investigatory Powers Act 2014 was then replaced by the Investigatory Powers Act 2016. Nevertheless, in April 2018, the UK High Court ruled that the Investigatory Powers Act 2016 violated EU law since access to retained data was not limited strictly to the purpose of combating "serious crime" and took place without a prior review by a court or another independent body. The Investigatory Powers Act must be re-drafted accordingly.[207]

4.3.3 The main regulatory actors concerned with privacy and data protection

Both EU (Article 8(3) CFR, Article 16(2) TEU, Articles 51-59 Regulation 2016/679) and CoE law (Article 15 of Convention 108+) require independent supervision as an essential mechanism towards effective enforcement of data protection rules.[208] The establishment of independent supervisory authorities at the national level, in the form of a National Data Protection Authority (sometimes also known as "National Data Protection Commissioner"), is mandatory. Both Regulation 2016/679 and Directive 2016/680 require that each Member State maintain a national institution upon its territory that ensures compliance with EU data protection law.

At the national level, the supervisory authorities are granted with proactive and preventive supervision competencies. They are competent to exercise investigation and intervention within their territory,[209] to provide advice to data controllers and subjects, to impose bans and administrative fines, to order the rectification or erasure of personal data and to initiate legal proceedings by referring a matter to

[202] Cameron, E. (2015), The Data Retention Saga: Dutch Court Declared National Data Retention Law Invalid, peacepalacelibrary.nl

[203] Odinot, G. et al. (2017), Organised Cybercrime in the Netherlands: Empirical findings and implications for law enforcement, Dutch Ministry of Justice.

[204] Ibid.

[205] Ibid.

[206] CJEU, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, Judgment of the Court (Grand Chamber) of 21 December 2016, Joined Cases C-203/15 and C-698/15.

[207] Cobain, I., UK has six months to rewrite snooper's charter, high court rules, The Guardian, 27 April 2018.

[208] Handbook on European Data Protection Law (2018).

[209] CJEU, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, Judgment of the Court (Third Chamber) of 1 October 2015, Case C-230/14.

Copyright © Cyber-Trust Consortium. All rights reserved.

the court. CJEU, with its case law, calls for a broad interpretation of the powers of the supervisory authorities.[210] The Regulation 2016/679 provides a general framework for cooperation between the supervisory authorities in cross-border cases of data processing, establishing a "one-stop-shop" mechanism, where the authority of the main or single establishment of the controller or processor is the lead authority of the cooperation scheme.[211]

At the European level, the European Data Protection Supervisor (hereinafter, EDPS) is the EU´s independent data protection authority, whose role is to supervise the EU institutions, bodies, offices, and agencies in order to ensure their compliance with data protection law. The rules for data protection in the EU institutions as well as the duties and powers of the Supervisor and the Assistant Supervisor and the institutional independence of the EDPS are laid down in the Regulation 45/2001, which is also currently under reform. The EDPS may, therefore, be contacted for queries and complaints concerning European research projects.

Moreover, the Regulation 2016/679 established the European Data Protection Board (hereinafter, EDPB), an EU body with legal personality, as successor to the Article 29 Data Protection Working Party established under the Data Protection Directive. EDPB, consisting of the heads of the national supervisory authorities and the EDPS, is entrusted with tasks, which can be summarised in three main categories: a. consistency - EDPB can issue legally binding decisions in order to ensure consistent application of the Regulation, which can be challenged before the CJEU; b. consultation - EDPB has an advisory role towards the Commission; c. guidance - EDPB, following Article 29 Working Party´s tradition, will continue issuing guidelines and recommendations, facilitating best practice.[212]

[210] Handbook on European Data Protection Law (2018).
[211] Ibid.
[212] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

4.4 Scope of application of European Data Protection Schemes

With respect to Cyber-Trust, the two main legislative initiatives that are likely to be relevant to the project are the GDPR and the Police Directive. National security is outside the scope of EU law. This is the reason why the processing of personal data for national security purposes is not within the scope of the General Data Protection Regulation or the Police Directive. As a result, the provisions of the GDPR and Police Directive were not designed to be applicable to processing by intelligence services.

4.4.1 Context in which the Regulation (EU) 2016/679 (GDPR) applies

The GDPR applies to the processing of all personal data of individuals residing in the EU Member States. It does not apply 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" which specifically includes "the safeguarding against and the prevention of threats to public security and the free movement of such data".[213] Nor does it apply merely personal or household actions with no connection to a professional or commercial activity.[214] Finally, like the Directive 2016/680, it does not apply to processing related to activities outside Union law, including activities concerning national security.

4.4.2 Context in which Directive (EU) 2016/680 applies

The Directive 2016/680 applies to specific data processing activities related to law enforcement. Notably, its scope is limited 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". As such, its scope does not encompass all data processing activities in the police and justice sectors but only that processing which is for the purposes enumerated. For the processing of personal data by "competent authorities" for other purposes, the GDPR applies. This, however, does not cover processing in the context of criminal court proceedings. Furthermore, it does not only apply to the police and justice sectors. "Competent authority" can mean "any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive,"[215] including private entities as well.

Furthermore, the Directive does not cover data processing in the course of an activity that falls outside the scope of European Union law. Activities that fall outside the scope of Union law include "activities concerning national security" and activities within the scope of Chapter 2 "Policies on border checks, asylum, and immigration" of Title V of the TEU. This can create some confusion on the applicability of this provision in countries where national law does not distinguish between national security and policing function.

Finally, it is important to note that as a Directive, it needs to be transposed into national law to have an effect in the respective Member State. This process of transposition allows for some variation along national lines whilst preserving the essential context of the directive concerned. The process was meant to be resumed in May 2018, however many states are still (as of August 2018) on the drafting phase. The transposition process will be discussed further in section 5.3.2.

5. Data protection requirements of the potential application to the Cyber-Trust project

This section describes key rules and principles that must be adhered to in all instances of data processing, including processing of personal data that may occur in the context of the Cyber-Trust project.

[213] Handbook on European Data Protection Law (2018).
[214] Ibid.
[215] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

5.1 5.1 Personal Data and Cyber-Trust

Since the Cyber-Trust project will deploy techniques which will engage a vast amount of data, it is likely that there will be moments when questions will arise as to whether particular data are personal or not. Thus, it is worthy to take a closer look as to what could amount to be personal data in this specific context.

"Online identifiers", for instance, include IP addresses and cookies but other factors may also lead to the identification of an individual, such as aggregate network indicators and network flow data. Even if someone´s name is not known, a combination of other identifiers may suffice to identify an individual.[216] It is underlined that information one holds may indirectly identify an individual and therefore could constitute personal data, even if additional information is needed.[217] That additional information may be information one already holds from other sources, or it may be information that one needs to obtain from another place.[218] Data may not relate to an identifiable individual when in hands of one controller but it may do in the hands of another, when in conjunction with additional information, for instance.[219]

In some occasions, it might be possible for someone to reconstruct the data in a manner that it can be related to an individual. In order to consider the probability for an individual to be identified, an assessment of the means that could be used "by an interested and sufficiently determined person", may be necessary, in combination with a continuous valuation of the changes in the likelihood of identification over time, as a result of technological development or other conditions. For that purpose, so as to determine whether or not a set of data relates to a particular individual, partners may need to consider:[220]

- the content of the data;
- the purpose they will process the data for; and
- the results of or effects on the individual from processing the data.

Even after all those assessments, there will possibly still be circumstances where it may be tough to determine whether data are personal or not. If in doubt, as a matter of good practice, the information should always be treated with the necessary care, by ensuring that a clear reason for processing the data does exist and, in particular, all necessary security measures and safeguards are in place. If personal data can be genuinely anonymised, then the anonymised data are not subject to the GDPR. Pseudonymisation measures can help reduce privacy risks, and they may constitute an appropriate safeguard under specific circumstances. However, pseudonymised data are still personal data.

In the Cyber-Trust project, the collection and sharing of cyber-threat intelligence information will take place in the deepnet web fora or marketplaces and clearnet social platforms. This information will be used to detect emerging threats, zero-day vulnerabilities and new exploits to IoT devices, by identifying social platforms and threads that host cyber-threat related criminal activities and by classifying and ranking those threats and cyber-attack related products across the various online communities (Task 5.1). Such information, which may characterize the device, the network, etc. include data about the integrity of a device's firmware and critical OS files, installed software patches, exposure to known vulnerabilities, network behavioural patterns (e.g. traffic volume and protocols), and services utilisation (Task 6.1).

More specifically, the cyberthreat intelligence data that will be collected, will be coming from three sources,[221] namely internal sources (host data sources, network data sources, forensic toolkits, etc), community sources (observed malicious sources or data, e.g. lists with blacklisted IP addresses or file names) and external sources (such as news feeds on cyberthreats, vulnerability advisories and alerts, automated tools of search, information on malware and intelligence acquired from the dark web). This vast amount of collected data may include, indicatively:

- device's firmware data,

[216] Handbook on European Data Protection Law (2018).

[217] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007, 01248/07/EN WP 136.

[218] Information Commissioner´s Officer (ICO), What is personal data, ico.org.uk.

[219] Ibid.

[220] Ibid. In general, ICO´s website offers detailed guidance and checklists, when issues arise in relation to personal data definitions.

[221] More information on the relevant cyberthreat intelligence sources in the context of Cyber-Trust, please see D2.2 Threat-sharing methods, comparative analysis, Section 4, Cyber-Trust.

Copyright © Cyber-Trust Consortium. All rights reserved.

- data relating to the operating system and critical software,
- system/network configuration files, audit and event logs,
- logs from IDS and network monitoring systems,
- CPU and RAM usage as well as ports and services,
- network activity including cover channel details.

The development of the Cyber-Trust prototype is likely to include trials and experimentation which may involve the processing of personal data, such as the web crawler which will be trained on real data coming from various sources. It is, therefore, essential to consider the application of personal data protection rules and principles both a. in the use of a Cyber-Trust prototype for matters of criminal proceedings, specifically to prevent, investigate, detect and prosecute criminal offences and b. the use of personal data for research purposes in the Cyber-Trust project. As indicated in the sections below, the potential application depends on each type of activity, and it should be taken carefully into account for the further assessment of the project, as further explained in section 5.3.

5.2 Data controllers and data processors

Article 4 GDPR defines data controllers and data processors as below:[222]

(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.

The distinction is of high significance for compliance because the GDPR treats the data controller as the principal party for taking care of responsibilities such as collecting consent[223] or managing consent-revoking requests of data subjects.[224] When a data subject wishes to revoke his or her consent, therefore, will contact the data controller to request the termination of the processing, even when the data are stored on servers owned by the data processor.[225] Upon receiving this request, the data controller would proceed with asking the data processor to remove the relevant data. Moreover, data controllers shall only hire data processors which are compliant with the GDPR requirements.[226] The GDPR, however for the first time, introduces direct obligations for data processors, meaning that processors may be subject to sanctions and claims by data subjects.

During the research phase, the researchers acting as data controllers, are obliged to implement technical and organisational safeguards on the basis of Article 24 GDPR.[227] Furthermore, they are free to interpret their obligations under Articles 89 regarding safeguards for scientific research and 32 concerning the security of processing with respect to the general data protection principles, however, in principle, they are obliged to carry out a data protection impact assessment to assess the risks for data subjects´ rights and possible mitigation measures, whenever for instance new technologies are used.[228] Specifically, Article 32 GDPR states that the controller has to take into "account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons".

[222] For example, if Company X sells widgets to consumers and uses Company´s Y email automation system to email consumers on their behalf and track their engagement activity, then with regard to such email activity data, Company X is the data controller, and Company Y is the data processor.

[223] Article 29 Data Protection Working Party Guidelines on Consent under Regulation 2016/679, adopted on 10 April 2018, 17/EN WP259 rev.01.

[224] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2018, 00264/10/EN WP 169.

[225] Handbook on European Data Protection Law (2018).

[226] Ibid.

[227] Maldoff, G., How GDPR changes the rules for research, 19 April 2016, iapp.org

[228] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

Article 89 introduces pseudonymisation as an appropriate safeguard, defined as the process, where: "personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately". The other proposition is to use anonymised data, "information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable".[229] However, it should be kept in mind that the process of anonymising personal data is considered processing and that true and full anonymisation may be tricky.

The Article 29 Working Party stated in that context that: "[…] data controllers should consider that an anonymized dataset can still present residual risks to data subjects. Indeed, on the one hand, anonymization and re-identification are active fields of research, and new discoveries are regularly published, and on the other hand even anonymized data, like statistics, may be used to enrich existing profiles of individuals, thus creating new data protection issues. Thus, anonymization should not be regarded as a one-off exercise, and the attending risks should be reassessed regularly by data controllers".[230]

To this direction, the GDPR introduced the notions of "data protection by design" and "data protection by default", meaning that the principles of the GDPR must be built into the design or architecture of the ICT systems, as discussed further in section 5.7 of this document. The GDPR also encourages the creation of codes of conduct with the guidance of the European Data Protection Board (Recital 78), which controllers and processors can use in order to self-regulate their processing, within the boundaries of the GDPR.[231]

Article 3 of the Directive 2016/680 defines controllers and processors, as follows:

(8) 'controller' means the competent authority 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;

(9) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Concerning the Cyber-Trust prototype, one thing to keep in mind is whether private sector businesses are identified as being within the scope of the Directive, especially when taking into account handling services contracted out from public sector authorities to the private sector agencies that might account as data controllers. It will be difficult, though, to verify whether these businesses are in scope without looking into their specific legal arrangements, because many private businesses may be data processors and not controllers and thus would not qualify as competent authorities, according to the Directive.[232] In a case-by-case analysis, contracts will need to be reviewed, in accordance with national law, in order to determine whether a private body processing personal data for a criminal law enforcement purpose, where public power or authority is given by statute, is a controller or a processor.[233]

5.3 The legal basis of the data processing

5.3.1 Regulation 2016/679 – the GDPR

Article 6 of the GDPR requires that the processing of personal data must have a legal basis to be lawfully processed. In order to comply with such requirements, personal data may be lawfully processed only on the basis of one of the following grounds:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

[229] Recital 26 of the GDPR.

[230] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014, 0829/14/EN WP216, p.11-12.

[231] Blockchain Bundesverband, Blockchain, Data Protection and the GDPR, 25 May 2018, p.9.

[232] UK Government services, Data Protection Bill: implementing the European Union Law Enforcement Directive No: HO0295, gov.uk, p.6.

[233] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular, where the data subject is a child.

With regards to the Cyber-Trust project, the two most relevant legal bases are (a) as described above, i.e. the consent of the data subject and (f) the existence of a legitimate interest. During the research phase, (a) consent will be the sole ground when research subjects are used to provide personal data, for example when filling in an expert questionnaire. After the research, (a) consent and (f) legitimate interest of the service providers may be relevant.

As for the first case, concerning the legal ground of consent, it should be noted from the start, that research occupies a privileged position within the Regulation. By adopting a "broad" definition of research, GDPR encompasses the activities of public and private entities alike, covering also technological development and demonstration (Recital 159).[234] A data subject´s consent is one way that a controller can process personal data, and must be freely-given, informed, specific to the processing purpose and unambiguous. Informed consent means that the data subject must be provided with information about the processing of her personal data, including at least: the name of the data controller; the processing purposes; the type of processing activities and data; the possibility to withdraw consent; the use of data for automated-based decision making and profiling (if applicable) and the likelihood of international transfers. All these requirements, however, may be proven challenging in the context of research because in accordance with Recital 33 "[i]t is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of collection".[235] Thus, it is of paramount significance to outline the research purposes as clear as possible and re-assess them regularly. Moreover, Recital 50 provides that further processing for research purposes should be considered compatible.[236]

According to Article 6(1)(f), processing is lawful if it is "necessary for the purposes of legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child". The ground of legitimate interest is applicable only if the three conditions described in this provision are met, namely:[237] a. the notion of necessity implies that the processing of the data is the most effective and least intrusive solution for the objective pursued; b. the controller or even a third party must have a real and present legitimate interest for the processing, which should be clearly articulated and permitted by the Union and national law; and c. a balancing exercise must take place between the legitimate interest and the fundamental rights and freedoms of the individuals whose data are processed, taking into account the safeguards put in place and the reasonable expectations of the data subjects, based on the existence or the absence of a relationship with the data controller. The more loose this relationship is, the more this balance will tilt towards the rights of the individual, because if data subjects do not reasonably expect their data to be processed for purposes other than for those initially collected, then the rights of the data subject could override the legitimate interest of the controller. Legitimate interest is not applicable during the research phase, because even if the two first conditions were met, the necessary relationship of proximity between the data controller and the data subjects is not present.

As for the second case, after the research phase, both the grounds of consent and legitimate interest may be relevant. Consent, for instance, will be seeked from the individual users of the Cyber-trust for having their

[234] Maldoff, G. How GDPR changes the rules for research, 19 April 2016, iapps.org
[235] Article 29 Data Protection Working Group, Guidelines on consent under Regulation 2016/679, Revised and Adopted on 10 April 2018, 17/EN WP259 rev.01, p. 28.
[236] Handbook on European Data Protection Law (2018).
[237] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller Under Article 7 of Directive 95/46/EC, 844/14/EN WP 217, adopted on 9 April 2014, p.33.

Copyright © Cyber-Trust Consortium. All rights reserved.

devices connected to the platform. On the other hand, Recital 49 GDPR concerning network and information security as overriding legitimate interest states: "The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned: for example, preventing unauthorised access to electronic communications networks and malicious code distribution and stopping "denial of service" attacks and damage to computer and electronic communication systems." The balancing test proposed by the Article 29 Data Protection Working Party can be used as guidance for the balancing between the legitimate interest of the Cyber-Trust prototype provider and end-user and the fundamental rights and freedoms of the concerned data subject.[238]
The use of a Cyber-Trust prototype by law enforcement for the detection, prevention and prosecution of malicious activity may be exempted from the field of application of the Regulation 2016/679 by Recital 19 which excludes its application to personal data being used in connection with police and criminal justice activities on grounds of public safety, public security, and public order. However, in this case, such processing may fall under the scope of Directive (EU) 2016/680, as described next.

5.3.2 Directive (EU) 2016/680 - the Police and Criminal Justice Data Protection Directive

The scope of Directive (EU) 2016/680, as stated earlier, covers 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. The Directive relies, to a great extent, on the principles contained in the GDPR. However, it does not contain the principle of transparency.[239] The reasoning behind this choice of the co-legislators is that the specific nature of security-related processing requires some level of flexibility. The principles of data minimisation and purpose limitation must also be applied with some degree of flexibility in the same context. This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/93/EU of the European Parliament and of the Council.[240]
It is essential to understand, that processing is not captured by the provisions specific to law enforcement simply because data are passed to a law enforcement agency. If the organisation holding the data is not processing it for law enforcement purposes, then it will not be covered by the law enforcement provisions. Once it is transferred, the competent receiving authority will then be processing it for the purposes of law enforcement, and consequently, the provisions of Directive 2016/680, as transposed to the Member State law will be applicable.[241]
In practical terms, the legal bases on which the processing of personal data is authorised under Directive (EU) 2016/680 are provided in Article 8 of the Directive. The processing of personal data by the competent authorities for the purposes specified is lawful only to the extent that the processing is necessary for the performance of a relevant task.
Nevertheless, this does not mean that law enforcement authorities can process personal data at will provided it is for the purpose of preventing crime. For the processing to be considered lawful, it needs to take place in accordance with the national law.[242] If there is no law authorising the data processing by the competent authority, it will not be lawful. Member States can authorise particular activities in their national legislations,

[238] Idem.
[239] Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (Directive 2016/680), 17/EN WP 258, adopted on 29 November 2017.
[240] Recital 97 of Directive 2016/680.
[241] Information Commissioner´s Office (ICO), Guide to law enforcement provisions, 7 December 2017, pdpjournals.com
[242] Handbook on European Data Protection Law (2018).

Copyright © Cyber-Trust Consortium. All rights reserved.

by putting in place additional requirements, such as consent.[243] In this case, the Member State must specify the purpose of the processing and the type of personal data to be processed.[244] In general, laws pertaining to privacy will still apply, including the requirements described in the case law of ECtHR in section 3.4.2.1. So far, this is the process of the transposition in some Member States,[245] which may be relevant for the Cyber-Trust project, concerning the key law enforcement data processing provisions:

i. Cyprus

A Working Group, with the cooperation of the relevant Ministries and the Data Protection Commissioner, is set to prepare the legislation. The draft is to be sent to the Parliament before the end of 2018.[246]

ii. Greece

The public consultation about the new draft law [247] was concluded in March 2018, creating a unified national legal framework concerning data protection. Nevertheless, as of August 2018, the draft law has not been yet voted upon. Once valid, the Greek law will stand in force in parallel with the GDPR and will transpose the Directive 2016/680 into national law, with small derogations and additional safeguards. The Greek legislator chose, instead of modifying existing laws, to transpose the proposed European framework in its whole in a common codification with the GDPR provisions. No specific time limit for storage of the data is set, which is open to be decided by other national laws.

iii. Italy

In March 2018 the Decree of the President of the Republic No. 15 of the 15th of January 2018 was published, concerning the implementation modalities of personal data processing principles for police and justice purposes and the implementation of the Directive 2016/680 in Italy.[248] The Decree did not include any provisions regarding metadata retention by internet and telecom operators for criminal law purposes.[249] The reasoning behind the choice of the legislator is the issue of retention is out of the scope of the Decree because a new data retention law passed in Italy in 2017 (Law No. 167/2017), aiming to fill the gap that the invalidation of the Data Retention Directive caused in 2014. Disregarding CJEU´s ruling, the law extended the limit, by providing a retention time of maximum 6 years in total.

The Decree of January 2018 furthermore explains which operators fall under the definition of law enforcement authority by providing two levels: the first, based on a competence criterion, i.e. all public agencies which are by national law competent to undertake police activities; [250] The second, based on the assignment criterion, i.e. all those bodies which are instead tasked to undertake such activities, extending the definition of police operator to cover also entities which are not by nature considered law enforcement agencies.

iv. Luxembourg

[243] Ibid.

[244] Ibid.

[245] European Commission, Transposition of the Directive (EU) 2016/680: State of play in the Member States, February 2018.

[246] Ibid.

[247] Greek Draft Bill for the transposition of the GDPR and the Directive 2016/680 in the Greek legislation available in Greek at: http://www.opengov.gr/ministryofjustice/wp-content/uploads/downloads/2018/02/sxedio_nomou_prostasia_pd.pdf [Accessed: 04.08.2018].

[248] Attuazione della direttiva UE 2016/680 del Parlamento Europeo e del Consiglio, del 27.4.2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, Gazzetta Ufficiale della Repubblica Italiana; Number: 119; 24.05.2018.

[249] Fantin, S. (2018), Law enforcement and personal data processing in Italy: implementation of the Police Directive and the new data retention law, DANTE project, kuleuven.be

[250] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

The Council of Government of Luxembourg approved a bill, with regard to the processing of personal data in criminal as well as national security matters. The Bill modified 12 different laws, in accordance with the Directive.[251]

v. The Netherlands

A draft bill was submitted in the Parliament on time.[252]

vi. United Kingdom

Although it is not yet clear how the legal regime will be shaped after Brexit, UK chose to transpose the Directive 2016/680.[253] The Data Protection Act 2018 received Royal Assent on 23 May 2018.[254] Part 3 of the Data Protection Act includes explicitly the rights to access, the right to rectification and of erasure as well as protection against automated decision-making. The Act, on the other hand, provides for restrictions on those rights, under the condition that it is necessary and proportionate to do so in order to:[255] "avoid obstructing an investigation or enquiry; avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; protect public security; protect national security; and protect the rights and freedoms of others."[256] The aforementioned restrictions can take place in accordance with the data protection principles.[257]

5.4 The data processing principles

The fundamental data protection principles are found in Article 5 of the GDPR and in the Convention 108+ in different Articles.[258] These key principles must be applied in all instances of processing of personal data to which the Regulation is applicable. Restrictions can only happen under the condition that they are provided for by law, pursue a legitimate aim and are necessary and proportionate in a democratic society. Such principles may be of relevance to Cyber-Trust, especially in relation to tools or technologies that may process personal data.

The general principles in GDPR, are as follows, with commentary, wherever deemed necessary, related to their interpretation in the law enforcement context, as shaped by the Directive 2016/680.

5.4.1 Lawfulness, fairness and transparency

Lawfulness requires that the processing is based on the consent of the data subject or another legal ground provided in the data protection legislation. In particular, for every processing activity in the Cyber-trust context (including every database that will be created, and any likelihood of interoperability among those databases), there should be a legal ground found in the Union or national law. In GDPR, those grounds are set out in Article 6. The principle of fairness can be explained as the reasonable expectation of the data subject to be able to fully understand what is happening with their data and that the controller is in a position to demonstrate full compliance with the existing legislation.[259] Transparency establishes the obligation of the controller to keep the data subjects informed about the risks of the processing, their rights and the rules applying to the processing of their data.[260]

[251] David, D., Bills designed to implement the General Data Protection Regulation in Luxembourg, 5 September 2017, castegnaro.lu

[252] European Commission, Transposition of the Directive (EU) 2016/680: State of play in the Member States, February 2018.

[253] UK Home Office, Dept for Digital, Culture, Media and Sports, Data Protection Bill Factsheet – Law enforcement processing (Clauses 29–81), gov.uk

[254] Data Protection Act 2018, Her Majesty's Stationery Office (HMSO); 2018, Chapter 12, 23 May 2018.

[255] UK Home Office, Dept for Digital, Culture, Media and Sports, Data Protection Bill Factsheet – Law enforcement processing (Clauses 29–81), gov.uk

[256] Ibid.

[257] Ibid.

[258] Handbook on European Data Protection law (2018),

[259] Handbook on European Data Protection Law (2018).

[260] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, 17/EN WP260.

Copyright © Cyber-Trust Consortium. All rights reserved.

Providing data subjects with the same level of protection with regards to their rights to information, access to, or erasure of personal data as foreseen in GDPR, concerning data processing for police and justice matters could hinder operations carried out for law enforcement purposes. Hence, the principle of transparency is not included in the Directive 2016/680.[261] Even though the Member States may restrict the data subjects' rights, for instance, to protect public security or prevent the obstruction of an investigation, they must guarantee that the processing for law enforcement purposes is lawful, meaning that it is necessary for the pursued objective, conducted by a competent authority and based on EU or national law.[262] Moreover, consent of the data subject can never in itself constitute a legal ground for the processing of data in the context of the Directive. Where the data subject is required to comply with a legal obligation, it should be understood that the data subject has no genuine and free choice.[263]

5.4.2 Purpose limitation

The principle of purpose limitation is one of the fundamental principles of the EU data protection law and requires that any processing must be carried out for a specific, well-defined purpose and only for additional purposes that are compatible with the initial purpose. Any new purpose which is not compatible with the original one or is different, requires its own legal basis. For example, the disclosure of personal data to third parties for a new purpose will most likely need an additional legal basis. In Article 5(1)(b) GDPR, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is always considered compatible with the original purpose. In that case, appropriate safeguards must be put in place, such as anonymisation, encryption or pseudonymisation and the data subject should be informed, as discussed in section 5.3.[264]

5.4.3 Data minimisation

Data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. By using privacy-enhancing technologies and privacy-friendly solutions, it is often possible to avoid the use of personal data or minimise the processing.[265]

5.4.4 Data accuracy

Controllers must take measures to make sure that the data they are holding is accurate and up-to-date, with respect to the purpose of the data processing. Inaccurate data must be corrected or erased without delay.

5.4.5 Storage limitation

Personal data must be erased or anonymised once they are no longer needed for the purposes which they were collected for. Article (5)(1)(e) GDPR provides that archiving data for public interest, scientific or historical purposes, or for statistical use, may be stored for more extended periods. This principle has to be taken carefully also into consideration in the police sector,[266] where national laws define different appropriate time periods for storage,[267] as analysed in section 4.3.2.4 of this document.

5.4.6 Data security: integrity and confidentiality

Appropriate technical and organisational measures should be taken so as to protect personal data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure, damage or access. This is

[261] Handbook on European Data Protection Law (2018), p.258.
[262] For more information, on the principle of transparency in the law enforcement context and recommendations to the Member States concerning restrictions to the data subjects´ rights, see: Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (Directive 2016/680), 17/EN WP 258, adopted on 29 November 2017.
[263] Ibid.
[264] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, adopted on 2 April 2013, WP203.
[265] Handbook on European Data Protection Law (2018).
[266] S and Marper v United Kingdom [2008] ECHR 1581.
[267]Article 5 Directive 2016/680.

Copyright © Cyber-Trust Consortium. All rights reserved.

particularly important where the processing involves transmission of data over a given network. Article 25 of the GDPR which addresses the issue of data protection by design, explicitly mentions pseudonymisation, as an example of appropriate technical and organisational measures. Other solutions include the storage of the data in a secure physical environment, layered logins and strong cryptography.[268] A regular review of the measures is also expected, while any personal data breaches must be notified to the national supervisory authority and in some situations, the data subject itself.[269]

5.4.7 Accountability

Both under EU and CoE law, the controller is responsible for and must be able to demonstrate compliance with all the aforementioned data protection principles. There are many ways that the controllers can ensure their compliance, for instance by implementing data protection by default and by design or designating a data protection officer.

5.5 Rights of the Data Subject

The right to access one´s own personal data and the right to rectification are enshrined in EU primary law and accurately, in Article 8(2) CFR. In addition to that, GDPR establishes a coherent legal framework which empowers data subjects with better control over their personal data, by recognising a detailed framework of rights. Similar safeguards are also included in the Directive 2016/680- and the Convention 108+ at CoE level. Member States enjoy a margin of discretion under GDPR to restrict obligations and rights, if this is a necessary and proportionate measure in a democratic society, for instance, for the protection of judicial investigations and proceedings. However, according to Article 23(2) of GDPR, as a minimum level of protection, the national law must respect the core of the fundamental rights protected by Union law. Here follows a brief overview of those rights.

It is to be noted that a controller may use pseudonymisation methods that prevent it from being able to re-identify a data subject, without collecting additional information. Article 11 acknowledges this situation and provides an exemption from the rights to access, rectification, erasure and data portability outlined in Articles 15 to 20.[270] The exemption applies only if “the controller is able to demonstrate that it is not in a position to identify the data subject” and, if possible, provides notice of these practices to data subjects. Given the material scope of Cyber-Trust, this exemption may be applicable in specific contexts.

5.5.1 The right to be informed of the processing of his or her personal data

Article 12, 13 and 14 of GDPR introduce the controller´s obligation to take appropriate measures to provide any information to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information about the processing shall be provided in writing, or by other means, including, where appropriate, by electronic means, without excessive delay or expense.[271] Based on CJEU´s case law,[272] the right to be informed can be limited for reasons of prevention, investigation, detection and prosecution of criminal offences, if a Member State has introduced such an exception in its national law. Moreover, Article 14(5)(b)-(e) of GDPR provides that in case where the data has not been obtained from the data subject, the obligation to inform them will not apply, if the provision of such information is impossible or disproportionate in particular in the context of public interest or research. Article 13(3) of the Directive 2016/680 provides the possibility to the Member States to include restrictions to the right to be informed, as long as such measures are necessary and proportionate om a democratic society, in order to avoid obstructing official inquiries and investigations or prejudicing the prevention, detection or prosecution of criminal offences, protect the public or national security and the rights and freedoms of others.

[268] Council of Europe, Opinion on the Data protection implications of the processing of Passenger Name Records, T-PD (2016) 18 rev, Strasbourg, 19 August 2016.
[269] Handbook on European Data Protection Law (2018).
[270] Maldoff, G., Top 10 operational impacts of the GDPR: Part 8 – Pseudonymization, 12 February 2016, iapp.org
[271] Ibid.
[272] CJEU, Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others, Judgment of the Court (Third Chamber), 7 November 2013, Case C-473/12.

Copyright © Cyber-Trust Consortium. All rights reserved.

5.5.2 The right to access his or her own personal data

Article 15 of GDPR provides that the data subjects shall have the right to obtain from the controllers confirmation as to whether personal data concerning him or her is being processed, and where that is the case, access to the personal data. This provision must be seen in the light of the principles of fairness, transparency and accountability, so the right to access must not be unduly restricted by time limits.[273] Where automated decision-making is carried out, including profiling, the general logic behind any decisions taken must be explained.[274] Concerning processing of personal data for law enforcement purposes, Article 14 of Directive 2016/680 provides similar restrictions as seen above in the right to be informed.

5.5.3 The right to rectify incorrect personal data

According to Article 16 GDPR, in respect of the principle of accuracy, the data subject has the right to request from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Given the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement. Concerning processing of personal data for law enforcement purposes, the right to rectification may be restricted for the same purposes as the rights to access and be informed.[275]

5.5.4 The right to erasure ("the right to be forgotten")

Article 17 of the GDPR grants the right to the data subject to have his/her personal data erased or deleted, without undue delay. The burden of proof that the data processing is legitimate will fall on the data controllers, as pursuant to the principle of accountability.[276] Once again, the GDPR outlines exceptions to these rights for reasons of compliance with a legal obligation, public interest or research purposes. For police and judicial matters, the controller can, instead of erasure, restrict the processing, when the accuracy of data cannot be ascertained, or the data constitutes evidence, which has to be maintained.[277]

5.5.5 The right to data portability

According to Article 20 GDPR, “the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.” Therefore, the controller should develop interoperable formats, to facilitate information sharing.[278]

5.5.6 The right to object to processing on legitimate grounds

Article 21 GDPR elaborates on the right to object; the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her. The data subject has the right to object not only relating to his or her particular situation but against profiling as well. Under GDPR, the burden of proof is again vested with the controller who must show compelling grounds for continuing the processing. Concerning research, the GDPR balances the requirements of scientific research and the right of the data subjects to object with specific safeguards and derogations in Article 89.[279]

Thus, the Union or national law may provide derogations to the right to object if the latter would render impossible or seriously impair the achievement of the research purposes, and if the research purposes could

[273] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, 17/EN WP260.
[274] Handbook on European Data Protection Law (2018).
[275] Article 16 (4) Directive 2016/680.
[276] Handbook on European Data Protection Law (2018).
[277] Article 16 (3) Directive 2016/680.
[278] Handbook on European Data Protection Law (2018).
[279] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

not be achieved without such derogation, as long as safeguards as provided in Article 89 paragraph 1 are put in place.[280] Therefore, the legislation will vary across the Member States and a case-by-case assessment will be necessary. As for the use of the Cyber-Trust prototype, network and information system security constitute, according to Recital 49 of the GDPR, an overriding legitimate interest, that could also pose restrictions to the data subject´s right to object, as also discussed in section 5.3.

5.5.7 The right not to be subject to an automated decision

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her, or similarly significantly affects him or her.[281] Nevertheless, such automated decision-making may be acceptable if it is necessary for the performance of a contract, if the data subject gave explicit consent, or if the decision-making is authorised by law and the data subject´s rights are appropriately safeguarded. Further discussion on the issue is to be found in section 6.3.2[282]

5.5.8 The right to a judicial remedy and the right to receive compensation in case of a breach

Where the data subject considers that his or her rights under GDPR have been infringed as a result of the processing of his or her personal data under a regime non-compliant with GDPR, he or she has the right to lodge a complaint with a supervisory authority or/and bring their case before a court. For the right to remedy to be effective, the Regulation gives individuals the right to receive compensation from the controller for material and non-material damages. In addition to that, Article 83 of the GDPR empowers Member States´ supervisory authorities to impose administrative fines, while Article 58 grants them with other corrective powers.[283]

5.6 Special categories of personal data (sensitive data)

In Article 9 of the GDPR (as well as in Article 6 of the Convention 108+), genetic and biometric data (where used for ID purposes) or personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, information about the health, sexual life or orientation are considered as special categories of data. Data belonging to hese categories could entail substantial risks to a person's fundamental rights and freedom, for instance, by increasing the riks of discrimination.[284]

Due to their nature, in principle, the processing of such data is forbidden. However, the paragraph 2 of Article 9 GDPR provides an exhaustive list of exemptions. For instance, processing is permitted if the data subject has explicitly consented or if it concerns data which have become explicitly and manifestly public by the data subject.[285] Such exemptions also include the case that processing is necessary in order to carry out obligations or exercise other rights in the employment, social security and social protection context, to protect the vital interests of a natural person, to establish legal claims, to use for medical purposes or research and for public interest reasons. Notably, in the case of public interest, Member States may introduce further exemptions.[286]

Under Convention 108+ personal data relating to offences, criminal proceedings and security measures are enlisted as special categories of data.[287] In GDPR, however, such data are simply covered under Article 10. The processing of such data may only take place under the control of an official authority or when the processing is allowed by EU or national law with appropriate safeguards in place. For the processing of

[280] Maldoff, G., How GDPR changes the rules for research, 19 April 2016, iapp.org
[281] Handbook on European Data Protection Law (2018).
[282] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 3 October 2017, 17/EN WP251rev.01.
[283] Handbook on European Data Protection Law (2018).
[284] Handbook on European Data Protection Law (2018).
[285] Ibid.
[286] Ibid.
[287] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

special categories of personal data, in the context of law enforcement, the Directive 2016/680 constitutes *lex specialis*.[288]

5.7 Data Protection by Design and by Default

The concept of Privacy by Design was first widely presented in the 1990s,[289] embedding privacy measures and privacy enhancing technologies (PETs) directly into the design of information technologies and systems. "PET stands for a coherent system of ICT measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system".[290]

In the data protection context, the General Data Protection Regulation for the first time addressed Data Protection by Design as a legal obligation for data controllers and processors, referring explicitly to data minimisation and the possible use of pseudonymisation.[291] In relation to that, it also introduced the obligation of Data Protection by Default, encouraging engineers to include protection of personal data as a default property of systems and services.[292] Data protection by Design and by Default are regarded as a many-sided notion, comprising of multiple technological and organisational elements, which integrate privacy and data protection principles in systems, devices and services.[293] Although some components can be generalised and used in different systems without significant alterations, most of them are contextual and depend on the specific circumstances of the processing, calling for the conduct of a specific privacy risk assessment both prior the decision towards the means for processing as well as at the time of the processing itself.[294]

Whilst not being the sole factor to be considered, the existence of measures to reduce the potential impact on individual privacy and data protection allows for an important possible contribution to the development and implementation of digital surveillance technologies determining the proportionality of a potential deployment. Where such techniques have been employed, the use of a surveillance system is more likely to be considered "proportional" in a broader range of contexts. Such techniques could *inter alia*, for example, involve ensuring that intrusion into someone´s privacy occurred only where it was absolutely necessary or that cyberthreat intelligence mechanisms would only be activated where activity likely to be criminal takes place.

The concepts of Data Protection by Design and by Default are particularly important in the design and development phases of every technological project related to the gathering of large amounts of information, which might contain personal data or might interfere one way or another with individuals´ private sphere.[295] If such safeguards are not already considered at the design stage, may put obstacles in engaging privacy enhancement tools in a later stage and effectively restrict the use of the tool to contexts that only involve extremely severe criminality or limit the range of its features.

---

[288] Ibid.

[289] Cavoukian, A. (2011), Privacy by Design: The 7 Foundational Principles, Information & Privacy Commissioner, Ontario, Canada, available at: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf [Accessed: 29.07.2018].

[290] Communication from The Commission to The European Parliament And The Council On Promoting Data Protection By Privacy Enhancing Technologies (PETs), COM (2007) 228 Final, Brussels, 2 May 2007.

[291] Recital 107 of the GDPR.

[292] In 2014 ENISA issued the Report on Privacy and Data Protection by Design, providing an inventory of existing privacy by design approaches, strategies, and technical building blocks of various degrees of maturity. In 2015 ENISA provided a specific Report on Privacy by Design in Big Data, aimed at analysing privacy by design strategies and tools in the era of big data analytics.

[293] See European Union Agency for Network and Information Security (ENISA), https://www.enisa.europa.eu/topics/data-protection/privacy-by-design

[294] European Data Protection Supervisor (EDPS), Jasmontaite, L. et al [Eds], Implementation of Data Protection by Design and by Default: Framing guiding principles into applicable rules, Vienna, 9 June 2017. The guiding principles also include a useful toolkit concerning the implementation of the two data protection schemes, as part of data controllers´ legal obligations under GDPR.

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

Copyright © Cyber-Trust Consortium. All rights reserved.

5.8 Transferring data across borders

The data protection framework recognises that free movement of goods, capitals, services and people within the internal market requires the free flow of data. However, it also assesses the risks that such free movement may entail for personal data. EU data protection law draws a distinction between transfers of data within the EU and transfers of data to third countries, i.e. outside the EU. It is worthy to mention that it is not yet clear what kind of regime will be agreed between UK and EU, concerning the free flow of data after Brexit.[296]

5.8.1 Within the EU

With respect to the GDPR, the flow of personal data throughout the EU must be free from restrictions and cannot be prohibited by law. Except for the EU Member States, the area of free flow is also expanded to Iceland, Liechtenstein and Norway. Specifically, flows of personal data within the EU for purposes related to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties are subject to Directive 2016/680.

5.8.2 Outside the EU

For transfers outside the EU to third countries or to international organisations, more stringent rules apply. The logic behind this legislative choice is that countries outside the Union may not have the same level of data protection in their law as the Member States. Hence, under EU law, there are in principle two ways for allowing such transfers, either on the basis of an adequacy decision (Article 45 of the GDPR) or in the absence of such a decision, where the controller or processor provides appropriate safeguards (Article 46 of the GDPR).[297] When neither the country ensures an adequate level of protection, nor the controller provides the required safeguards, personal data can be transferred to third countries only if additional conditions are met (Article 49 of the GDPR).[298]

[296] Ibid.

[297] Several types of such appropriate safeguards exist.

[298] Article 29 Data Protection Working Party, Guidelines on Article 49 of Regulation 2016/679, adopted on February 2018, 18/EN WP262; European Data Protection Board (EDPB), Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018.

Copyright © Cyber-Trust Consortium. All rights reserved.

Part C – Cybercrime and cybersecurity

6. Network and Information Systems Security

6.1 CoE Legal framework – The Convention on Cybercrime

The Convention on Cybercrime of the Council of Europe,[299] known as the Budapest Convention, is the only binding international instrument on this issue. The Budapest Convention is supplemented by a Protocol on Xenophobia and Racism committed by means of computer systems. The Cybercrime Convention Committee (T-CY), the monitoring body of the Convention in 2012 decided to issue Guidance Notes aimed at facilitating the use and implementation of the Budapest Convention on Cybercrime.[300]

The offences under the Convention can be groupped into: "a. offences against the confidentiality, integrity and availability of computer data and systems; b. computer-related offences; c. content-related offences; and d. criminal copyright infringement."[301] Under the Additional Protocol, the act of using computer networks to publish xenophobic and racist propaganda constitutes a criminal offence. However, it is noted that the full range of cybercrimes is not covered under the Budapest Convention. For instance, identity theft, sexual grooming of minors and unsolicited spam are not included.[302]

Moreover, the treaty provides a model for mutual information sharing and formal assistance among law enforcement agencies.[303] Article 23 of the Convention outlines the general principles for international cooperation in criminal matters related to computer systemas and the collection of electronic evidence, while Article 39 of the Convention states that the provisions only supplement multilateral and bilateral treaties already effective between parties. The adoption of the Convention aims to enhance harmonisation of the different national legislations and leads to reciprocal criminalisation.[304]

The Convention on Cybercrime has come under severe criticism mainly for two reasons. First, some of its provisions allegedly fail to protect effectively rights of individuals and second, it is considered in general inadequate to ensure a cyberspace free of criminal activity, by failing to address the needs of modern investigation or even supposedly infringing on state sovereignty.[305] Brazil, China, Russia and India are non-signatory parties of the Convention.

6.2 EU Legal framework

6.2.1 The Directive 2013/40/EU on attacks against information systems

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[306] introduces rules to counterforce attacks against information systems. Illegal access, system interference or interception constitute criminal offences across the EU. The aim of these new rules is the same as the one pursued by the Cybercrime Convention: to harmonise the criminal law of the Member States in the area of attacks against information systems and to reinforce cooperation between Member States' law enforcement authorities.

[299] Council of Europe, Convention on Cybercrime, 23 November 2001, CETS No.185.
[300] Weber, A. M. (2003), The Council of Europe's Convention on Cybercrime, 18 Berkeley Tech. L.J. 425.
[301] Ibid.
[302] Ibid.
[303] Gercke, M. (2012), ITU publication - Understanding cybercrime: phenomena, challenges and legal response, Telecommunications Development Sector, p.11.
[304] Ibid, p.11.
[305] Council of Europe, Cybercrime Convention Committee (T-CY) T-CY, Guidance Note #3: Transborder access to data (Article 32), 3 December 2014, Strasbourg: "In particular, Article 32 has been contentious as it allows local police to access servers located in another country's jurisdiction, even without seeking sanction from authorities of the country. In order to enable quick securing of electronic evidence, it allows trans-border access to stored computer data either with permission from the system owner (or service provider) or where publicly available".
[306] 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.

Copyright © Cyber-Trust Consortium. All rights reserved.

On the definition of relevant terms, the Directive refers to:[307]

- "Information system" in Article 2(a): The definition is similar to the definition of a computer system as provided by Article 1(a) of the Budapest Convention, but computer data are explicitly covered by the Directive as well.
- "Computer data" in Article 2(b): The definition follows Article 1(b) of the Budapest Convention, referring to an information system instead of a computer system.
- "Legal person" in Article 2(c): The definition covers both natural and legal persons from a liability perspective. States, public bodies or international public organisations are excluded.
- "Without right" in Article 2(d): The definition addresses a general principle of criminal law and aims to avoid criminal liability for individuals acting either in accordance with domestic law or with the authorisation of the owner/another right holder of the information system or part of it.

New criminal offences are defined, as follows:[308]

- Illegal access to information systems in Article 3;
- Illegal system interference in Article 4: The Directive lists eight possible acts, namely inputting computer data, transmitting, damaging, deleting, deteriorating, altering or suppressing such data, rendering it inaccessible and two possible results of the respective act, namely severely hindering or interrupting the functioning of an information system;
- Illegal data interference in Article 5, which refers to any unlawful interference with computer data impairing its integrity or availability;
- Illegal interception of non-public transmissions of computer data and electromagnetic emissions from an information system carrying such data in Article 6;
- Illegal provision of tools used for committing the aforementioned offences in Article 7: In this context, such tools could be a computer programme, a computer password or any other data allowing access to an information system.
- The criminal liability is also extended to incitement, aiding and abetting by natural and/or legal persons to commit as well as their attempt to commit an offence, in Article 8. Inciting, aiding and abetting cover all the offences referred to in Articles 3 – 7, whereas the attempt refers only to Articles 4 and 5.

Minimum levels of penalties for offences referred to in the Directive are provided for in Article 9. Taking into account that the offences mentioned above can be committed in one place while their effects might take place in another, Article 12 provides for obligations to establish jurisdiction based upon: a. the place where the offender is physically present when committing the offence, b. the location of the targeted information system, c. the nationality of the offender, d. the offender´s habitual residence, and e. the place of establishment of a legal person for whose benefit the offence is committed. Concerning exchange of information, Article 13(1) requires the Member States to establish national operational points of contact, which will be available 24 hours a day 7 days a week and will be expected to reply to urgent requests within 8 hours after they have been addressed with a request.

6.2.2 The Directive 2016/1148/EU concerning measures for a high common level of security of network and information systems across the Union - The NIS Directive[309]

The Directive 2016/1148/EU is the first attempt for a European legislation on cybersecurity.[310] The Directive 2016/1148/EU (hereinafter, NIS Directive) was adopted by the European Parliament in July 2016 and entered

[307] European Commission, Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Brussels, 13.9.2017 COM (2017) 474 final, p.4.

[308] Ibid.

[309] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30.

[310] European Commission, The Directive on security of network and information systems (NIS Directive), available at: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive [Accessed: 02.08.2018].

Copyright © Cyber-Trust Consortium. All rights reserved.

into force in August 2016. On 30 January 2018, Commission Implementing Regulation (EU) 2018/151 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact was adopted.[311]

According to the Directive, Member States should develop a national cybersecurity strategy; designate a national authority in charge of the implementation of the Directive, and to establish a national single point of contact; determine one or more computer security incident response teams (CSIRTs); and furthermore implement specific security requirements and other obligations for Operators of Essential Services (OESs) and Digital Service Providers (DSPs).[312] The NIS Directive provides security requirements for IT systems, regardless of whether personal data are affected. The Member States must put in place "effective, proportionate and dissuasive" sanctions for infringement cases.[313] Since its scope of application includes both operators of "essential services" and "digital service providers", EU Member States must determine which organisations are subject to the rules, since different obligations are foreseen for OESs and DSPs.

Operators of Essential Services (OESs) are required to "take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems" and "appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services".[314] OESs have to report "incidents having a significant impact on the continuity of the essential services they provide without undue delay to competent authorities or CSIRTs set up by each Member State". According to the Directive, there are seven sectors of essential services, these being energy, transport, banking, financial market infrastructures, health, potable water supply and distribution, and digital infrastructures.

Digital Service Providers (DSPs) - online marketplaces, online search engines and cloud computing service providers - also have obligations to safeguard the security of their network and information systems and minimise the impact of security incidents. [315] Member States cannot increase these requirements, except for reasons of national security or justice matters, but they can place more strict obligations on OESs.[316] DSPs, like OESs, are required to notify incidents that have a "substantial" impact on their offered services in the EU without undue delay.[317]

6.3 At the Member State level

In order for the Cyber-Trust project to achieve an effective design, it will have to determine early in time its area of action, in other words the type of cybercrimes that it will try to detect and mitigate, taking into account what is accepted as cybercrime in the different jurisdictions, where the system will be deployed and that not all types of what is commonly accepted as "cybercrime" in non-legalese are prosecuted.

Therefore, in this section, we will examine what is the state of the national legislation concerning cybercrime and cybersecurity, based on the obligations introduced by the CoE Cybercrime Convention and the above EU Directives, with emphasis on Directive 2013/40/EU since the NIS Directive still requires acts from the side of the Member States in order to be fully transposed. As a general observation, Member States had to transpose the NIS Directive into their national laws by 9 May 2018 and identify operators of essential services by 9 November 2018. However, due to the fact that a large number of states failed to communicate any

[311] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, C/2018/0471, OJ L 26, 31.1.2018, p. 48–51.

[312] Kalis, P., NIS Directive – update for the Netherlands, Leiden Law Blog, 31 January 2018.

[313] Article 21 NIS Directive.

[314] Article 14 NIS Directive.

[315] Recital 49 NIS Directive.

[316] Article 1 NIS Directive.

[317] Article 16 NIS Directive.

Copyright © Cyber-Trust Consortium. All rights reserved.

implementation measures by the May deadline, the European Commission sent in July 2018 a letter of formal notice to 17 Member States to fully comply with their obligations under EU law.[318] Italy, Cyprus and UK have already transposed the NIS Directive into national law, whereas the drafting of the relevant legislation is still in progress in Greece, The Netherlands and Luxembourg. Nevertheless, most of the Member States have already adopted National Cybersecurity Strategies.

i. Cyprus

The primary laws in the field of cybercrime are:[319]

- The Law 22(III)/2004 ratifying the CoE Convention on Cybercrime (Budapest Convention). The Additional Protocol to the Convention on Cybercrime, concerning the Criminalization of Racist and Xenophobic acts was also ratified by Law 26(III)/2004.
- Law 112(I)/2004 regulating Electronic Communication and Postal Services.
- Law 183(I)/2007 on the Retention of Telecommunication data for the investigation of serious offences, which transposed the Data Retention Directive. Even though the Directive was invalidated by the Court of Justice of the EU, the national law is still valid.
- Law 91(I)/2014 that revises the legal framework on the prevention and combating sexual abuse and exploitation of children and child pornography. This legislation ratified the EU Directive 2011/93/EU and covers child pornography, grooming and notice and takedown.
- Law 147(i)/2015, transposing the Directive 2013/40/EU on attacks against information systems. The adopted legislation covers all the definitions in the Directive 2013/40/EU and refers explicitly to the criminal offences of illegal access being committed by infringing a security measure, and of the illegal system interference. Concerning the transposition of Article 5 (illegal data interference) and Article 6 (illegal interception), Cyprus used in its legislation the same text as in the Directive.[320]

The National Cybersecurity Strategy, the main instrument for coordinating the national efforts against cybercrime, was adopted by the Ministerial Council in 2018, in accordance with the requirements set out in the NIS Directive. The Office of the Commissioner of Electronic Communications and Postal Regulations is responsible for its implementation and monitoring. The NIS Directive was implemented with the Law 17(I)/2018 of 5 April 2018 on Network and Information Systems Security.[321] With this law, Cyprus adopted the definitions of OESs and DSPs presented in the NIS Directive and established its competent national authority, opting for a centralised model (Articles 2 and 3 of Law 17(I)/2018). The CSIRT will be part of the competent authority and will receive guidance and oversight (Article 3 of Law 17(I)/2018).

ii. Greece

An overview of the Greek Laws and Presidential Decrees applicable in the case of cybercrime is, as follows:[322]

- Law 2121/1993 “Intellectual property, related rights and cultural issues”;
- Law 2225/1994 “For the protection of freedom of response and communication” as amended until today;
- Law 2867/2000 “Organisation and operation of the Telecommunications sector”;
- Presidential Decree 47/2005 “Procedures and technical and organisational provisions to intercept the secrecy and security of communication”;

[318] European Commission, Fact Sheet - July infringements package: key decisions, Brussels, 19 July 2018, available at: http://europa.eu/rapid/press-release_MEMO-18-4486_en.htm [Accessed: 27.08.2018].

[319] Crime Combating Department, Relevant Legislation, available at: http://www.police.gov.cy/police/police.nsf/All/D753CDF2D439A9EAC225829C003B75D4?OpenDocument [Accessed: 06.08.2018].

[320] More information on EUR-LEX, available at: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32013L0040 [Accessed: 30.08.2018].

[321] The relevant legislation in Greek may be found here: http://www.cylaw.org/nomoi/arith/2018_1_017.pdf [Accessed: 27.08.2018].

[322] Papathanasiou, A. et al. (2014), Legal and Social Aspects of Cyber Crime in Greece, E-Democracy, Security, Privacy and Trust in a Digital World (5th International Conference, E-Democracy 2013, Athens, Greece, 5-6 December, 2013), Revised Selected Papers, Volume 441.

Copyright © Cyber-Trust Consortium. All rights reserved.

- Presidential Decree 150/2001: "Digital Signatures";
- Presidential Decree 131/2003: "Electronic commerce etc."
- Law 3471/2006 "Protection of personal data processing and private life in the sector of telecommunications – Amendment of Law 2472/1997" and the forthcoming Law transposing GDPR and the Directive 2016/680 into domestic legislation;
- Law 3431/2006 "Electronic communications and other issues";
- Law 3674/2008 "Strengthening the institutional framework to protect the privacy of telephone communication and other issues";
- Law 3783/2009 "Identification of owners and users of mobile telephone services and other issues";
- Law 3917/2011 "Retention of telecommunication data and other issues".

Until recently, the Greek Criminal Code (GCC) did not include any laws referring exclusively to the internet and relevant criminal activities. General criminal laws applied, along with the so-called "special criminal laws". In 2016, the Law 4411/2016 on the ratification of the CoE Convention on Cybercrime and the transposition of the Directive 2013/40/EU came into force. The Law brought, *inter alia*, the following changes in the Criminal Code.[323]

Whoever, without right, gains access to whole or part of an information system may be sentenced to imprisonment.[324] In the case of critical infrastructures, the imprisonment may be at least 2 years.[325] The investigation and prosecution of such an offence are subject to a complaint by the victim.[326] The aforementioned provisions of the Criminal Code make hacking/cracking of any sort without permission, irrespective of any intention or damage, illegal. This way, even minor attacks are criminalised. Relevant criminal offences are also covered in Article 292a of the Criminal Code. According to this Article, access without right to a connection or network of telephone communications or a software system is criminalised, as well as access without right to a network of electronic communications.[327]

Whoever without right seriously hinders or interrupts the functioning of an information system (DoS & DDoS, as well as acts of hacktivism) by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, is punishable as a criminal offence, with imprisonment.[328] If the interference caused serious damage, the offender is sentenced to at least 1 year of imprisonment.[329] If the crime was committed by an organised team[330] or against critical infrastructure, the offence is punished with stricter sanctions.[331] Identity theft, following the Cybercrime Convention paradigm, is not included as an offence against the functioning of an information system.

Deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data unusable or inaccessible, intentionally and without right, is punishable as a criminal offence, with at least 3 years of imprisonment.[332] Depending on the damage caused[333] or on whether the crime was committed by an organised crime group, or against a critical infrastructure, the gravity of the offence would be different.[334] The aforementioned crimes are dependent on a complaint by the affected victim.[335] These provisions criminalise attacks with viruses and malicious software.

[323] More information on EUR-LEX, available at: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32013L0040 [Accessed: 30.08.2018].
[324] Article 370c para 1 GCC.
[325] Articles 370c para 2 GCC and 3 of the Directive 2013/40.
[326] Article 370c para 3 GCC and Article 3 of the Directive 2013/40.
[327] Article 370a GCC.
[328] Articles 292b para 1 GCC and 4 of the Directive 2013/40.
[329] Articles 292b para 2 GCC and 4 of the Directive 2013/40.
[330] Articles 292b para 3 GCC and 4 of the Directive 2013/40.
[331] Articles 292b para 4 GCC and 4 of the Directive 2013/40.
[332] Articles 381a para 1 GCC and 5 of the Directive 2013/40.
[333] Articles 381a para 2 and para 3 GCC, and 5 of the Directive 2013/40.
[334] Articles 381a para 5 GCC and 5 of the Directive 2013/40.
[335] Articles 381a para 6 GCC and 5 of the Directive 2013/40.

Copyright © Cyber-Trust Consortium. All rights reserved.

Whoever intercepts, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right, in order for them or someone else to have illicit knowledge of the intercept content,[336] may be sentenced maximum 10 years.[337] Concerning illegal interception, the Greek law requires special intention, in other words, to gain knowledge, have economic gain, or cause disadvantage.

The intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and within the intention for it to be used for the commitment of cybercrimes as described in the previous articles, and in particular:[338]

(a) a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 292b and 370b, 370c και 370d:

(b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

Therefore, the aforementioned provisions criminalise the preparatory acts of criminal acts, such as the use of botnets. In order for the research in the field of security of information systems to stay outside the scope, the creation and use of such tools is only criminalised if there is an intention for them to be used for the commission of criminal acts. So scientists or white hat hackers who check the security of a system for purposes of research or with specific permission, are excluded.[339] Last but not least, offences of using information systems for sexual grooming of minors and computer fraud, including the interference without right with an information system or accessing information, which are capable of causing monetary damage, were also included in the Criminal Code with the Law 4411/2016.

As for the implementation of the NIS Directive, Greece has adopted its cybersecurity strategy and has taken actions to implement the rest of the points raised in the text of the Directive, working towards the adoption of a legal framework.[340]

iii. Italy

Concerning the transposition of the Directive 2013/40/EU, which was transposed in the Italian legislation in 2015 and introduced 39 amendments in existing laws, similar terminology is used to describe the criminal offence of illegal access.[341] Concerning the use of criminalised tools, though, the new provisions require specific intent to inflict damage or to act fraudulently. Concerning illegal interception, the Italian legislation excludes from its application the electromagnetic emissions.[342]

Moreover, the Italian Criminal Code and special laws on copyright and the protection of credit cards cover all the offences under Articles 2-10 of the Budapest Convention.[343] Under Articles 24 and 24bis of Legislative Decree no. 231 of 8 June 2001, a provision has also been made for the liability of legal persons for commission of some cybercrimes for their own benefit. The Ministerial Decree of 28 April 2008 has set out specific investigative areas of competence for the Post and Communications Police in the field of critical computerised infrastructures and the regularity of telecommunication services, online child pornography and intelligence gathering for cybercrimes related to the illicit use and forgery of means of payment. Under Article 2 of Decree-Law of 18 February 2015 no. 7, converted with amendments into Law no. 43 of 17 April 2015,

[336] Relevant crimes are included in the Article 292a, 370a, 370b και 370c GCC, in Article 15 of the Law. 3471/2006 concerning the protection of electronic communications and the Article 10 of the Law 3115/2003 for the confidentiality of communications.

[337] Articles 370d para 1 GCC and 6 of the Directive 2013/40.

[338] Articles 292c para 1 GCC as well as 370e para 1, and Article 7 of the Directive 2013/40.

[339] Recital 17 of the Directive 2013/40.

[340] Maglaras, L. et al. (2018), NIS directive: The case of Greece in Security and Safety.

[341] More information on EUR-LEX, available at: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32013L0040 [Accessed: 30.08.2018].

[342] Council of Europe, Status regarding Budapest Convention – Italy, coe.int

[343] Law of 22 April 1941, no. 633 on Copyright, that also lays down criminal sanctions in relation to alleged violations on the Internet (Article 171 et seq.); Criminal law protection of credit cards under Article 55 of Legislative Decree of 21 November 2007 no. 231.

Copyright © Cyber-Trust Consortium. All rights reserved.

the role of the Post and Communications Police was reinforced in the fight against terrorism, including the internet. Last but not least, the Electronic Communications Code (Legislative Decree 1 August 2003, no. 259) includes the related obligations for Italian telecommunications companies.

In February 2017, the Italian Council of Ministers adopted a Decree on cyber protection and on national cybersecurity as a first step to transpose the NIS Directive, which further reinforced the role of the Inter-ministerial Committee for the Security of the Italian Republic in implementing cybersecurity measures described in the Directive, and provided guidelines to increase the level of cybersecurity in the country.[344] In May 2018, the Italian Government adopted the Legislative Decree 65/2018, eventually transposing the Directive, without, however, finalising its implementation process since Italy must still update its national cybersecurity strategy and regulate the regime of its CSIRT.[345]

The Decree entered into force in June 2018 and followed the scope of the Directive entirely, identifying the competent Authorities and their respective tasks.[346] Concerning which OESs and DSPs are covered under the Decree, Italy sticks to the NIS Directive recommendations. The Decree repeats the same general security requirements laid down by the NIS Directive to be taken into consideration by OESs and DSPs and requires and establish their duty to notify, without undue delay, alleged security breaches to the national CSIRT. With regard to the national authorities in charge of the implementation of the Decree and the supervision of its compliance, Italy chose a decentralised sector-by-sector model, led by five Ministries. In case of breach of obligations, the competent authorities may impose administrative fines up to 150.000 Euros.

iv. Luxembourg

The most relevant piece of law in Luxembourg is the Act of 18 July 2014 on Cybercrime, transposing the Directive 2013/40/EU and introducing into national law the amended Directive on the protection of private life and electronic communications.[347] The Budapest Convention was ratified a year later.[348] Other documents relevant to cybercrime are: [349]

- The Luxembourgish Criminal Code;
- The Luxembourgish Code of Criminal Procedure;
- The Law of 15 July 1993 aimed at reinforcing the fight against economic crime and computer fraud;
- The Law of 14 August 2000 on electronic commerce;
- The Law of 18 April 2001 on copyright, neighbouring rights and databases;
- The amended Law of 30 May 2005 establishing specific rules for the protection of privacy in the electronic communications sector.

Concerning the transposition of the Directive 2013/40/EU, the scope of the national legislation is broader, with regards to illegal access to information systems. Article 7 of the Directive criminalises a number of acts concerning tools such as computer programmes or access codes for committing the offences mentioned in Articles 3-6: the production of such tools, their sale, procurement for use, import, distribution or otherwise making available. The Luxembourgish legislation criminalises all acts related to the creation and use of such tools. As for Illegal data interference, the Luxembourgish legislation covers only some of the alternative acts described in Article 5 of the Directive.

[344] Guastamacchia, F. (2017), The role of blockchain in revolutionizing and re-organizing security: Evidence and policy recommendations, LUISS Universita Guido Galli, p.51.

[345] Cyber Security and NIS Directive: the Italian implementing Decree, 29 June 2018, blblex.it

[346] Ibid.

[347] 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.34.

[348] More information on EUR-LEX, available at: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32013L0040 [Accessed: 30.08.2018].

[349] Computer Incidence Response Center, TR-44 - Information security - laws and specific rulings in the Grand Duchy of Luxembourg, circl.lu

Copyright © Cyber-Trust Consortium. All rights reserved.

As for the implementation of the NIS Directive, in March 2015 Luxembourg adopted its updated Cybersecurity Strategy,[350] while in June 2018 the government announced the first steps towards its transposition into Luxembourgish Law, with the modification of the Law of 23 July 2016 creating the Haut-Commissariat à la Protection Nationale, as well as the modified law of 20 April 2009 establishing the Centre de Technologies de l'Information de l'Etat.[351]

v. The Netherlands

In order to comply with its obligations under the Cybercrime Convention, the Dutch Criminal Code included, under the Computer-crime Law (CC-II) in 2006, the following crimes as defined by Articles 2-6 of the CoE Cybercrime Convention: [352] illegal access, unlawful interception, data manipulation, computer sabotage. Articles 7 and 8 of the Cybercrime Convention were already implemented as follows: forgery of documents, according to Dutch legislation a document includes an electronic document as well. Computer fraud was covered by traditional provisions. Offences related to infringements of copyright and related rights were covered by the Copyright Act (Auteurswet 1912). Attempt, aiding and abetting was covered explicitly, while corporate liability is covered by general provisions.

Concerning the transposition of the Directive 2013/40/EU, the adopted in 2015 legislation follows the proposed terminology by the Directive to describe the criminal offence of illegal access.[353] As for illegal data interference, the Dutch legislation covers only a few of the alternative acts described in Article 5 of the Directive, whereas interception of electromagnetic emissions is not considered illegal. Other cybercrimes as laid down in the Directive (hacking and spamming, illegal distortion of data and illegal interception of data) were already implemented in the Dutch legislation, as seen above thanks to the Computer-crime Law of 2006. Penalties were also increased to 2 years imprisonment, in accordance with the obligation in Article 9 of the Directive. Furthermore, aggravating circumstances were added to the Dutch Criminal Code that lead to a maximum imprisonment of 3 years in case of deploying "botnets" and to 5 years in case of committing a cybercrime causing "serious damage", or against the information system of a "vital infrastructure". It is up to the judiciary, however, to decide what should be considered "serious damage", since the Directive did not give any definition on that matter and the Dutch law did not include any, either.

The investigation, prosecution and punishment of crime in The Netherlands are governed by the Code of Criminal Procedure, which sets the procedures for dealing with different types of offences. Nevertheless, the Dutch parliament is considering two new laws that would expand the capabilities of the intelligence and security communities and provide them with additional tools and authorities to investigate and combat advanced cyberattacks. On the one hand, the Data Processing and Compulsory Reporting Cybersecurity Act (Wet Gegevensverwerking en Meldplicht Cybersecurity) would increase the police's authority to detect serious cybercrimes. On the other, the new Computer-crime Act III (Wet Computercriminaliteit III) would grant special powers to police and other investigative services to remotely infiltrate – or hack – the computers of suspects under certain conditions. The law requires from the police to immediately disclose any software vulnerability discovered, including zero-day vulnerabilities, to the software developers. Both laws have already passed in the House of Representatives but have yet to be voted upon in the Senate.

As for the implementation of the NIS Directive, the transposition of the Cybersecurity Law – (Cybersecuritywet (Csw)) is still in progress and it is going to repeal the existing law of 1 October 2017 (Wgmc) regarding the processing of data and the duty to report cybersecurity, which covers many of the topics introduced with the NIS Directive.[354] Nevertheless, the Dutch cybersecurity agenda was adopted and

[350] The text of the National Cybersecurity Strategy II can be found here: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf

[351] For more information, see: https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-rna-nis-directive-implementation-luxembourg-law-12062018.pdf

[352] Council of Europe, Status regarding Budapest Convention – The Netherlands, coe.int

[353] More information on EUR-LEX, available at: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32013L0040 [Accessed: 30.08.2018].

[354] European Commission, Implementation of the NIS Directive in The Netherlands, available at: https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-netherlands [Accessed: 28.08.2018].

Copyright © Cyber-Trust Consortium. All rights reserved.

published earlier in 2018,[355] and the National Cybersecurity Strategy was already introduced in 2011 and updated in 2013.[356]

vi. United Kingdom

The extensive legislation in the UK on cybercrime includes *inter alia* the Computer Misuse Act 1990, the Police and Justice Act, the Serious Crime Act, the Terrorism Act, the Regulation of Investigatory Powers Act, the Telecommunications Regulations and the Data Protection Act 2018. The UK ratified the Budapest Convention in 2011. The British law makes a distinction between a cyber-enabled crime and a cyber-centric crime. Cyber-centric crimes include crimes brought about due to the existence of computers, whereas cyber-enabled crimes have always existed but nowadays are greatly facilitated by computers, such as fraud.[357]

The Computer Misuse Act 1990 (CMA)[358] constitutes the central piece of UK legislation relating to cyber-crimes such as hacking and DoS attacks.[359] The 1990 Act does not define what is meant by a "computer", to allow for technological development. It describes three offences: a. unauthorised access to computer material, b. unauthorised access with intent to commit or facilitate the commission of further offences, c. unauthorised acts with intent to impair, or with recklessness as to impairing, the operation of the computer, etc. The 1990 Act has been amended twice, by the Police and Justice Act 2006 and by the Serious Crime Act 2015. Two more offences were added: d. unauthorised acts causing or creating a risk of, serious damage and, e. making, supplying or obtaining articles for use in cybercrimes – intent is not required in that case. The offence (d) is the most serious crime covered by this Act and has a maximum sentence of life, whereas the other offences carry a different potential prison sentence, ranging from 2 years to 10 years.

The changes introduced by the Serious Crime Act in 2015 were aimed to cover partly the requirements of the EU Directive 2013/40/EU.[360] Moreover, the Computer Misuse Act was amended in a way to include offences which are committed even by suspects who are located outside of the UK at the time of the offence, insofar as the act is illegal in that country too and the offender is a UK national.[361] The Police and Justice Act amended the Computer Misuse Act to include: "unauthorised acts with intent to impair the operation of a computer" which adds DoS attacks as an offence, even if the disrupt is only temporary. According to the Terrorism Act 2000: "[An offence is committed if the action] is designed seriously to interfere with or seriously to disrupt an electronic system".[362]

Lastly, concerning the requirements laid out in the NIS Directive, the Digital Charter, as of January 2018 brings together a broad, ongoing programme, which will evolve as technology changes, including stricter guidance for cybersecurity policies.[363] The UK Network and Information Systems Regulations 2018 (the NIS Regulations) came into force on 10 May 2018 to transpose the NIS Directive.[364] The NIS Regulations 2018 impose obligations to OESs, who operate in the fields of energy (electricity, oil and gas), transport (air, rail, water and road), health (hospitals, private clinics and online settings), digital infrastructure (domain name registries, service providers and internet exchange points) and water (drinking water supply and distribution) (Article 8 NIS Regulations). Nevertheless, appropriate authorities also retain a discretionary power within their sectors to designate an organisation as an OES, where a cyber incident affecting that organisation would likely have a significant disruptive effect on the provision of essential services. As DSPs qualify providers of

[355] The Dutch Cybersecurity Agenda, available in Dutch: https://www.nctv.nl/ncsa/index.aspx [Accessed: 28.07.2018].

[356] Information was taken from: https://hollandfintech.com/2018/03/fight-cybersecurity-netherlands/ [Accessed: 28.08.2018].

[357] Graceful, H., UK Cyber Crime Law, 15 June 2016, gracefulsecurity.com

[358] The Crown Prosecution Service, Computer Misuse Act 1990 - Legal Guidance: Cyber / online crime, cps.gov.uk

[359] Cyber Crime And Security – House Of Commons Library. (n.d.), available at: https://commonslibrary.parliament.uk/key-issues/cyber-crime-and-security/ [Accessed: 20.08.2018].

[360] More information on EUR-LEX, available at: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32013L0040 [Accessed: 30.08.2018].

[361] Uk Cyber Crime Law — Gracefulsecurity, available at: https://www.gracefulsecurity.com/uk-cyber-crime-law/ [Accessed 20.08.2018].

[362] Ibid.

[363] Kalis, P., NIS Directive – update for the Netherlands, Leiden Law Blog, 31 January 2018.

[364] The legislation is available online at: https://www.legislation.gov.uk/uksi/2018/506/made

Copyright © Cyber-Trust Consortium. All rights reserved.

online marketplaces, online search engines or cloud computing services as long as the head office is established in the UK or they have appointed a legal representative, and do not fall under the definition of micro or small enterprises.

The NIS Regulations impose two categories of duties to OESs and DSPS: an obligation to take appropriate and proportionate measures to ensure security and a duty to notify the competent authorities in case of a security breach. In relation to the security measures, the UK government has adopted a principles-based approach, rather than prescriptive rules. As for the obligation to notify, OESs are obliged to report to the competent authorities any incident that "has a significant impact on the continuity of the essential service which that OES provides", while DSPs are obliged to notify "any incident having a substantial impact on the provision of any of the [relevant] digital services…", without undue delay and no later than 72 hours after the incident came to their knowledge (Articles 11 and 12 of NIS Regulations). As for which authorities qualify as competent, UK followed a decentralised sector-by-sector model, rather than appointing one central competent authority (Schedule 1 of NIS Regulations) and can impose a financial penalty up to £17m (Article 18 of NIS Regulations). Information sharing among the competent authorities can occur if it is necessary and proportional to the requirements of the NIS Regulations (Article 6 of NIS Regulations).

6.4 Special issues in relation to network & information system security

With the reformed data protection package entering into force only a few months ago and a rather quick change being witnessed in the digital ecosystem, there is still some obscurity as for how specific notions will be implemented and interpreted until the courts start delivering their first decisions on cases being brought before them. Thus, it is considered handy to address a couple of specific issues which might create data protection concerns and other legal implications during the creation and implementation of the Cyber-Trust project, within the context of cyberthreat intelligence gathering for the detection and mitigation of cyberattacks.

6.4.1 Web crawling and data scraping

For the end-users of a Cyber-Trust prototype are not identified yet, it is deemed necessary to discuss the issue of the use of web crawling and screen scraping tools both under GDPR and in police and criminal justice context. As of today, there is no specific law defining the legal status of scraping or prohibiting it altogether. However, such tools do not only raise concerns of data protection and privacy in its broader sense, as seen in the relevant section 3.4.2.2 but also issues which are covered by other fields of law, more specifically intellectual property rights, as recently shown in the CJEU case law. Since the amount of information being scraped is enormous, the theoretical possibility that this information may contain personal data cannot be excluded. Moreover, this collection and storage of an individual´s information, which would often happen without her knowledge could raise an issue of data protection.[365] In that case, as well as in case of doubt, the controller will need to ensure that the processing is compliant with the relevant data protection legislation.

The use of web crawlers, as an automated investigatory measure for intelligence and law enforcement purposes, brings the question of authorisation.[366] Such automated measures must be authorised by domestic or EU law, and its deployment must be carried out in accordance with those laws.[367] [368] However, when crawling takes place on restricted access sources,[369] will most likely require prior judicial authorisation or at least a kind of authorisation by the owner of the source, in line with the data protection and privacy framework.[370] Depending on the country where the investigation is conducted, accessing restricted fora

[365] Rubinstein, I.S. Big Data: The End of Privacy or a New Beginning? In International Data Privacy Law, 2013, Vol. 3, No. 2, pp.74-87.
[366] Recital 35 Directive (EU) 2016/680.
[367] Zouave, E. (2017), Law Enforcement Webcrawling: Lawfulness by Design and by Default, DANTE project, KU Leuven CiTiP.
[368] Article 8 ECHR; Article 7 CFR.
[369] eg. Twitter feed.
[370] Zouave, E. (2017).

Copyright © Cyber-Trust Consortium. All rights reserved.

could be as well considered an interception of content data or a seizure of computer data.[371] Moreover, as for the access to open sources, since the use of web crawlers could cause DDoS or severely affect the availability of a service, a prior risk assessment may have to take place and a permission for jamming communications may be necessary in some jurisdictions.[372]

Nevertheless, information acquired with these methods still poses legal challenges, which will be briefly introduced in Part D of this document. The legal uncertainty that arises from using new investigatory technologies can be reduced if privacy and data protection by design and by default are implemented, as discussed in section 5.7.[373] In the case of the web crawling for the creation and use of the Cyber-Trust prototype, it must be ensured that personal data that may be found during the searches are obtained by lawful means by the organisation that provided the data to the specific website, on an appropriate legal ground (such as consent, legal obligation, public or legitimate interest of the controller) and that the data shared via the portal or website are proportionate. A case-by-case analysis is particularly important regarding web crawling for data "available in the public" since harvesting data via web-crawlers raises very significant questions concerning necessity of the processing as well as the reasonable expectations of the data subjects, purpose limitation and accuracy of a database populated in such a manner.

Although not related to data protection, another legal issue could arise. The CJEU held that the scraped non-creative content but rather factual data from a company´s website were not protected by intellectual property rights and therefore another organisation scraping their data did not infringe upon the company's intellectual property.[374] The CJEU emphasised, however, that it is possible for a website owner to restrict the re-use of the mined data through the terms of use applicable to his or her website.[375] Therefore, if someone accesses a website, consenting to the terms of use which enclose a restriction on the re-use of data, any subsequent re-use may hold them liable for breach of contract.[376]

All in all, although there is no specific law against scraping or using publicly available information which has been obtained through the use of automated scraping tools, the user may be held liable if the scraping and subsequent use of the scraped information infringes the website owner's intellectual property rights or, if the user violates the terms of use of the specific website.[377] Again an assessment of whether there is an infringement or not will take place on a case-by-case level, in particular with regards to searches in the dark web.

6.4.2 Profiling of IoT devices and blacklisted IP addresses

The Internet of Things (IoT) is understood to be "a global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities. This infrastructure includes existing and involving internet and network developments. It will offer specific object-identification, sensor and connection capability as the basis for the development of independent cooperative services and applications. These will be characterised by a high degree of autonomous data capture, event transfer, network connectivity and interoperability."[378] Technological advances and improvement of the capabilities of big data analytics, artificial intelligence and machine learning nourish profiling and automated decision making with the potential to impact individuals' rights and freedoms significantly.

The Cyber-Trust project aims to collect and evaluate information that may characterize IoT devices and the relevant network in general; examples include information about the integrity of a device's firmware and

[371] Ibid.

[372] Ibid.

[373] Article 20 Directive (EU) 2016/680.

[374] CJEU, Ryanair Ltd v PR Aviation BV, Judgment of the Court (Second Chamber), 15 January 2015, Case C-30/14.

[375] Rezai, A., Beware of the Spiders: Web Crawling and Screen Scraping – the Legal Position, 6 February 2017, parissmith.co.uk

[376] Ibid. The UK Supreme Court took a different approach to the CJEU in NLA v Meltwater (2013) where it was held that Meltwater's use of news headlines, scraped from news websites as links to the relevant news articles amounted to copyright infringement.

[377] Rezai, A. (2017).

[378] Ibarra-Esquer, J.E. et al (2017), Tracking the Evolution of the Internet of Things Concept Across Different Application Domains, in Sensors.

Copyright © Cyber-Trust Consortium. All rights reserved.

critical OS files, whether software patches have been installed, exposure to known vulnerabilities, network behavioural patterns (e.g. traffic volume and protocols), and services utilisation. This information will have as a result the profiling of devices, with signs of alleged past, present or future malicious activity. There is the theoretical possibility that the device profiling could lead to the profiling of the individual user, in particular with the storage of data on a platform with blacklisted devices and IPs. Since the possibility of false positives cannot be excluded, it is worthy to examine the implications of such a scenario.

The relevant legal framework to assess privacy and data protection issues raised by the IoT in the EU is composed of GDPR as well as specific provisions of the e-Privacy Directive.[379] Article 6 GDPR provides the lawful bases for processing in the context of profiling or automated decision making. In the case of Cyber-Trust, Article 6(1)(a) and 6 (1)(f) are the grounds with the most relevance, as also seen in section 5.3.

The GDPR defines profiling in Article 4(4) as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[380] It is clear that the choice of the wording suggests that profiling involves some form of assessment or judgment.

Automated decision-making, on the other hand, has a different scope and may partially overlap with or result from profiling.[381] Strict automated decision-making is the ability to make decisions based on technological means without any human involvement. Automated decisions can be based on any type of data, thus if the data used in an automated decision-making or profiling process is inaccurate, any result, decision or profile will be flawed.[382] As a result, any platform of profiled or blacklisted devices or IP addresses which will be created in the Cyber-Trust project needs to be kept up-to-date and accurate, to as great an extent as possible. The finding of a correlation does not entail that this correlation is significant or relevant. As an automated process only make assumptions about an individual´s behaviour or characteristics, errors cannot be eliminated, and therefore, a balancing exercise is needed to weigh the risks of using these results. Profiling techniques carry potential dangers because they are often invisible to individuals, who might not expect such a process or may not be capable to comprehend how the process works and in what way this process can affect them. Moreover, the decisions taken may lead to significant adverse effects for some individuals.[383]

Article 22(1) of the GDPR narrows the circumstances in which solely automated decisions can be taken, including decisions based on profiling, that can have a legal or similarly significant effect on individuals. When human involvement is required, this has to be active and not just symbolic. The question is whether a human reviews the decision before it is implemented and has the discretion to alter it, or whether a person blindly applies the decision taken by an automated system. If the process is fully automated, due to the high risk that the processing poses to the individual, a data protection impact assessment should take place before any decision is made.[384]

If the Cyber-Trust prototype is used for law enforcement and justice matters, then the specific domestic laws will have application in this respect. Nevertheless, based on the Opinion of Article 29 Working Party on the Directive 680/2018, "[t]he general prohibition on 'solely automated' 'individual decision', including profiling, having an 'adverse legal effect' or 'significantly affecting' the data subject should be respected. It is important to highlight that a typical adverse effect resulting from automated decisions could be the application of increased security measures or surveillance by the competent authorities."[385] National laws providing exceptions to this prohibition must provide suitable safeguards for the rights and freedoms of data subjects,

[379] Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 September 2014, 14/EN WP 223.

[380] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 3 October 2017, 17/EN WP251rev.01.

[381] Ibid.

[382] Ibid.

[383] Ibid.

[384] Ibid.

[385] Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (Directive 2016/680), 17/EN WP 258, adopted on 29 November 2017.

Copyright © Cyber-Trust Consortium. All rights reserved.

including the right to obtain human intervention, in particular, to express his or her point of view, to obtain an explanation of the decision or to challenge it.[386]
To ensure privacy requirements while still supporting accountability, the data collected by the Cyber-Trust platform will have to be secured with all the necessary and appropriate safeguards.

6.4.3 Deep Packet Inspection and network traffic

When a user transmits a communication via the internet, this transmitted information is divided into packets,[387] which are transmitted across the internet from the sender to the recipient, including among others, information about the source and the destination. Each packet has two parts, the IP payload that includes information, which is addressed only to the recipient, in other words, the content of the communication.[388] The second part of the packet is the IP header that includes, among others, the address of the recipient and the sender. ISPs and other intermediaries ensure that IP packets travel across the network through nodes that read the IP header, till their final destination. Such protocols use common agreed language to carry the communication, and once the package has been forwarded to the next node, the router does not need to keep the information any longer.[389]

This network traffic can be analysed, for different purposes, with the use of inspection techniques, characterised by a different level of intrusiveness.[390] In Cyber-Trust, a deeper packet inspection will be likely applied. In that case, the researcher may access the information which is addressed to the recipient of the communication, depending on the deep packet inspection techniques that will be used. With the help of these tools, ISPs and researchers can, for instance, block web traffic or detect illegal content. Inspection techniques based on IP headers and in particular, those using deep packet inspection involve the monitoring and filtering of vast amounts of data and have severe implications in terms of privacy and data protection, as well as confidentiality of communications.
Depending on the goals pursued with the monitoring and interception, it is not the same to merely inspect communications, for example, to ensure the proper functioning of a system or the identification of a malware, and to deeply inspect communications in order to determine whether restrictive policies must be applied or for behavioural advertising.[391] The difference is observed on the fact that the latter measure may have a more imminent impact on individuals.[392] The correct application of monitoring, inspection and filtering techniques must be conducted in compliance with the data protection and privacy framework, which lays down boundaries as to what can be done and under which circumstances. Under data protection legislation, the processing of personal data, such as in this case the processing of traffic and communication data, requires an adequate legal ground,[393] alongside with specific requirements for special types of personal data. The content of communications and the traffic data are both protected by the confidentiality of correspondence, guaranteed by Article 8 ECHR and Article 7 and 8 of the Charter. Predominantly, Article 5(1) of the e-Privacy Directive regarding the confidentiality of communications requires the Member States to assure the confidentiality of communications and of the related traffic data by means of a public communications network and publicly available electronic communications services. At the same time, Article 5(1) of the e-Privacy Directive foresees that the processing of traffic and content data by ISPs may be allowed, in certain circumstances, with the consent of the users. The listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, is prohibited, except when ISPs are legally authorised to do so

[386] Ibid.
[387] European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data, 11 October 2007.
[388] Ibid.
[389] Ibid.
[390] Friedewald, M. J. [ed.] et al. (2017), p.87.
[391] European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data, 11 October 2007, para 78 and 79.
[392] Friedewald, M. J. [ed.] et al. (2017), p.88.
[393] European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data, 11 October 2007.

Copyright © Cyber-Trust Consortium. All rights reserved.

in accordance with Article 15(1). Except for the consent of users concerned, the e-Privacy Directive foresees other grounds that may legitimise ISPs' processing of traffic and communications data. The relevant legal grounds for processing, in this case, are: a. delivering the service (Article 6(1) and (2)); b. safeguarding the security of the service (Article 4); and c. minimising congestion (Article 5 and Recital 22).[394]

Concerning safeguarding the security of a service, an ISP is under a general obligation to take appropriate measures to secure the safety of the network it operates.[395] Therefore, an ISP can engage in monitoring and filtering, as well as other traffic management policies, insofar as it respects the boundaries of proportionality and data minimisation and follows strict limitations on the retention and processing of the collected data, in line with Articles 4 and 6 of the e-Privacy Directive.[396] Both principles oblige ISPs to refrain from monitoring of the content of individuals´ communications that entail processing of excessive amount of information or has benefits for ISPs only. Thus, ISPs must *a priori* assess the techniques to be used, the level of intrusion, the desired results and the specific privacy and data protection safeguards in place.[397] If the same results can be achieved with less intrusive techniques, then the less intrusive means should always be preferred. Pseudonymisation and anonymisation, as appropriate safeguards, must also be considered.

As for minimising congestion, Recital 22 to the e-Privacy Directive explaining the Article 5(1), does not prohibit any automatic, intermediate and transient storage in so far as it takes place for the sole purpose of carrying out the transmission and does not last longer than necessary.[398] In parallel, the confidentiality of the communications must be guaranteed. Provided the overall societal interest in efficient communication, ISPs may argue that prioritising or slowing down traffic to address congestion is a legitimate measure which is necessary to deliver an adequate service. However, in that case, the principle of proportionality and data minimisation should be taken again into account.[399]

Although it is important to notice that the transposition of the e-Privacy Directive into the national legislations may differ and thus, the following observation may not apply in a particular case under a specific jurisdiction,[400] inspection and further use of traffic and communication data for purposes other than those described above is only permitted under strict conditions, in compliance with Article 5(1) of the e-Privacy Directive which requires consent from users concerned to listen, tap, store or engage in other kinds of surveillance or interception of communications and the related traffic data. Recital 17 of the e-Privacy Directive states that "[...] Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website". Consent is not considered to have been given freely if the individual had to consent to the monitoring of their communication data in order to get access to a communication service.[401] In reality, determining in which cases consent is necessary, and in which cases, for instance, the security of the network is an overriding interest, is not an easy exercise, in particular, if the purposes of the inspection techniques are bifold.[402]

Moreover, consent must be obtained from all users involved in a communication, because the latter traditionally takes place between at least two parties.[403] Nevertheless, when monitoring and intercepting traffic and communications, for example, web traffic, it may be enough for ISPs to obtain the consent of their subscriber.[404] However, the situation may be more complicated when the sender or the recipient do not both

[394] Ibid.
[395] Ibid.
[396] Ibid, para 78, 79 and 80.
[397] Ibid.
[398] Ibid, para 42.
[399] Ibid, para 44.
[400] For instance, in Greece, inspection and further use of traffic and communication data for purposes other than those that are being described into the Act 3471/2006 (the one that implements the ePrivacy Directive) fall under the Data Protection Regulation (i.e. in GDPR now)
[401] European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data, 11 October 2007, para 55.
[402] Ibid, para 50 and 56.
[403] Ibid, para 64.
[404] Ibid, par 65.

Copyright © Cyber-Trust Consortium. All rights reserved.

have a contractual relationship with the same ISP or when more individuals use the same household communication network permanently or occasionally.[405] Again, a case-by-case assessment is required.
In derogation from Article 6 of the e-Privacy Directive, traffic data can be exceptionally retained for a limited period based on Member States´ legislation.[406] Retention, as seen above, is only allowed when it constitutes a necessary, appropriate and proportionate measure within a democratic society which aims to safeguard national security, state defence, public security, and assist with the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications.[407]

[405] Ibid.
[406] Ibid.
[407] Article 15 para 1, e-Privacy Directive.

Copyright © Cyber-Trust Consortium. All rights reserved.

Part D – Electronic (or digital) evidence[408]

7. Rules and principles governing the use of electronic evidence in criminal proceedings

The aim of the Cyber-Trust project is to develop a prototype that will not only be capable of detecting possible threats but also to provide material that will potentially be stored in blockchain and be used as evidence in criminal proceedings. In order to be able to make use of the material in such a way, the concerned data will have to be handled in a manner that is not only consistent with laws that have already been described in this document, but also with rules concerning, in specific, the gathering and use of evidence in criminal proceedings. So as for Cyber-Trust to be suitable for its desired use, it is equally important to consider this second category of laws.

Admissibility of electronic evidence in criminal proceedings depends on: a. general rules and principles concerning due process in criminal proceedings; b. general rules of evidence in criminal proceedings and; c. specific rules relating to electronic evidence in criminal proceedings.[409] Each of these are considered in the following sub-sections of this document. Level of protection differs from jurisdiction to jurisdiction. For instance, in some legal systems, evidence needs to be legally obtained, i.e. by a Court Order, in order to be admitted before a Court.

It will be necessary for those partners involved in the design of the Cyber-Trust prototype to embrace these principles so that the created tool is, to as great an extent as possible, capable of promoting good practices with regards to the gathering and use of evidence. Since the handling and use of electronic evidence is the subject of the deliverable D3.2, only a general overview of the main points in relation to the topic is included, as follows.

7.1 General rules concerning Due Process in criminal proceedings

In the criminal proceedings, on the one hand, stand the defendants, usually a private individual with minimal resources[410] and on the other the state and its sophisticated and complex criminal justice machinery, including *inter* alia the police, the administrative criminal justice system and the prisons. Given this disparity of resources, there would be little chance of a fair hearing unless rules existed to restrain the state and ensure that it operates in a proper way, for instance by only presenting evidence that is real, accurate, lawfully acquired, related to the given question before the court.[411] The idea of "due process" in that case guarantees that proper procedures exist so as to make sure that evidence is collected, processed and presented in a sound way to the courts and that the defendant´s right to a fair trial is well respected.[412]

The Universal Declaration of Human Rights states in Article 10 that "everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him". The right to be presumed innocent is dealt with in Article 11 Universal Declaration of Human Rights (UDHR). The right to a fair trial, including the right to be presumed innocent has been translated into obligations in a number of international and regional human rights instruments, such as Article 14 and Article 15 ICCPR, Article 6 and Article 7 ECHR and Articles 47 to 50 of the EU Charter of Fundamental Rights. Specifically, Article 6 of the European Convention on Human Rights, which is binding in most European legal systems and has been in the epicentre of the case law of the ECtHR, states:

[408] The terms "electronic evidence" and "digital evidence" are in legal literature and practice used interchangeably. However, for reasons of consistency, in this document only the term "electronic evidence" will be used.

[409] See: "The Admissibility of Electronic Evidence in Court: Fighting Against High Tech Crime" created within the context of the CYBEX initiative concerned with the Admissibility of Electronic Evidence in Court. Available at: https://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf

[410] Jackson, J. and Summers, S, (2012), The Internationalisation of Criminal Evidence.

[411] Quinn, P. (2016).

[412] Ingle, J. (2014), Overview: Criminal Law, Evidence and Procedure, Cambridge Journal of International and Comparative Law 3, pp. 265-268.

Copyright © Cyber-Trust Consortium. All rights reserved.

1. *In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly, but the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.*
2. *Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law*
3. *Everyone charged with a criminal offence has the following minimum rights:*

(a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
(b) to have adequate time and the facilities for the preparation of his defence;
(c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;
(d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
(e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

Whereas Article 6 guarantees the right to a fair hearing, it neither contains explicit mentions concerning the gathering of evidence, nor it provides specific rules that are applicable to the admissibility of it.[413] The Strasbourg Court, though, has stated that such specific rules are a matter of national law[414] and that the question to be answered in that case is that of whether the proceedings were as a whole fair, including an assessment of the way evidence was obtained. There is a number of implicit general principles which the ECtHR has recognised to apply on the handling of evidence in criminal proceedings, contributing to the interpretation of the relevant domestic law.[415] [416] Those principles, as read below, might be of importance for the Cyber-Trust prototype, once its use cases are defined:

Fairness: It is crucial that in "determining whether the proceedings as a whole were fair, to examine whether the rights of the defence were respected. In particular, it must be checked whether the applicant was given an opportunity to challenge the authenticity of the evidence and to oppose its use."[417] The principle of fairness entails that any evidence must have been collected in a fair manner, in other words, in a lawful way and without violating the rights and freedoms of the defendant. Otherwise, the proceedings may be regarded as violating Article 6, irrespective of whether the evidence holds truth.[418]

Quality: In criminal proceedings, the reliability or accuracy of evidence play a significant role, when assessing the quality of it, and consequently its admissibility. The Court attaches particular weight to whether the evidence in question was decisive for the outcome of the proceedings.[419] Where the quality of the evidence in question is weak, supporting evidence of another kind should also be required.[420]

Appropriate oversight: Whilst the ECtHR has accepted the possibility of covert surveillance activities, given the fact that such activities might infringe upon individual rights, they should be supervised by proper monitoring authorities be it a judge or a prosecutor.[421]

Issues related to entrapment: The Strasbourg Court in its case law admits that competent authorities can use special investigative methods and that covert digital surveillance itself does not infringe upon the right

[413] Fair Trials International, Third Party Intervention in the ECtHR, Application No. 30460/13, March 2014.
[414] ECtHR, Schenk v. Switzerland, para 45-46; Heglas v. the Czech Republic, para 84.
[415] For a detailed analysis: Council of Europe/European Court of Human Rights, Right to a fair trial. Article 6 of the Convention – Criminal law, 2014.
[416] Quinn, P. (2016).
[417] Council of Europe/European Court of Human Rights, Right to a fair trial. Article 6 of the Convention – Criminal law, 2014, p 24.
[418] ECtHR, Jalloh v Germany, para 105.
[419] ECtHR [GC], judgment of 1 June 2010, Gäfgen v. Germany, appl. no. 22978/05.
[420] ECtHR, judgment on Merits and Just Satisfaction of 2009, Bykov v Russian Federation, appl. no. 4378/02.
[421] ECtHR, judgement of 4 November 2010, Bannikova v. Russia, appl. no. 18757/06.

Copyright © Cyber-Trust Consortium. All rights reserved.

to a fair trial.[422] The rise of organised crime, in particular, requires that states take appropriate measures to face the emerging challenges. However, the right to a fair trial, having such a vital position in a democratic society must apply to all types of crime, ranging from the simplest to the most complex, without exceptions.[423] In this context, the Court has stated that the police whilst permitted to act undercover may not act in a way that is intended to incite criminal activity.[424]

7.2 The European legal framework on electronic evidence

7.2.1 From conventional to digital

Many of the laws and the related jurisprudence pertaining to evidence date back to an era when the criminal investigation was relying on the conventional means of gathering and analysing physical evidence.[425] However, nowadays, conventional crimes can be committed in virtual environments or produce digital evidence of high significance, while new forms of criminal activity emerge, leaving behind various digital traces. For this reason, digital forensics[426] have been developed as a sub-branch of forensics, and digital means of investigation increasingly gain popularity and relevance.[427]

For gathering electronic evidence can be done covertly, remotely, and with the help of powerful automated tools without necessarily any human intervention, balancing the need to guarantee efficient criminal prosecution on the one hand, and guaranteeing sufficient protection of each individual's fundamental rights on the other, requires safeguards of a different nature than those required for conventional investigations.[428] Not only do technically different methods of gathering evidence require different safeguards, but also the different degrees of the data subject's exposure will need to be taken into account in any proportionality analysis.

For the investigation of the relevant crimes, enforcement authorities have in their disposal a variety of powers, ranging from interrogations and surveillance to search and seizure of stored computer data, real-time collection of network traffic data, computer files, logs, metadata, and so on. The collected data might or might not be relevant to the crime under examination, whereas in most of the cases they will give comprehensive insights into both the private and perhaps professional life of the data subject and their peers. Therefore, when electronic evidence is gathered, and personal data are likely to be involved directly or indirectly, the general data protection principles, which were presented in section 5.4 of this document must be taken into account. Although these principles are not particular to electronic evidence, they have been widely incorporated in the relevant existing and under discussion European legal frameworks. New data protection risks emerge, especially regarding online environments and communications, which have not yet been addressed explicitly by the legislator, in particular wherever existing law seems to have been established considering the physical evidence only, and therefore not taking into account particular privacy risks related to electronic evidence.[429]

Electronic evidence is defined as "any information (comprising the output of analogue devices or data in digital format) of potential probative value that is manipulated, generated through, stored on or communicated by any electronic device".[430] This broad definition, refers to various categories of data in

[422] ECtHR [GC], Ramanauskas v Lithuania, judgment on Merits and just satisfaction of 5 February 2008, appl. no. 74420/01.

[423] Council of Europe/European Court of Human Rights, Right to a fair trial. Article 6 of the Convention – Criminal law, 2014, p 25.

[424] ECtHR, judgment of 26 October 2006, Khudobin v Russia, appl. no. 59696/00.

[425] Quinn, P. (2016).

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

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

[428] Quinn, P. (2016).

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

[430] EVIDENCE project, European Informatics Data Exchange Framework for Courts and Evidence, D3.1 Overview of existing legal framework in the EU Member States. There are various definitions of electronic evidence, but the definition provided by the Evidence project is preferred, because of its broad scope.

Copyright © Cyber-Trust Consortium. All rights reserved.

electronic form that is relevant in investigating and prosecuting criminal offences — including "content data" for instance e-mails, text messages, videos and photographs – often stored on the servers of online service providers -, as well as other types of data, such as subscriber data or traffic information regarding an online account. However, it could also include conventional evidence which is somehow digitised.[431]
The processing of evidence in criminal cases includes the collection, preservation, use, exchange and transfer of evidence.[432] What is meant by collection of electronic evidence, also in relevance for Cyber-Trust project, is the process of gathering material of any type that contains potential electronic evidence in the broadest sense, including search, seizure, interception and any other forms of gathering performed by Law Enforcement Agencies (LEAs), but also capture of data from the private sector, for instance ISPs, or by individuals, that could later be used for legal proceedings. Preservation aims to secure the integrity of the evidence, with the use of a suitable storage method. Transfer of electronic evidence may occur within the same country among different stakeholders in the field of police and justice cooperation, or between two competent authorities in different countries.[433] All the actions taking place from the very moment of the collection until the use of the evidence at court require a legal basis.[434]
Given the nature of electronic evidence, risks are higher with regards to the fair management and admissibility of evidence, including falsifying, destroying and manipulation of evidence. The complexity of electronic evidence entails that is not only the risk of falsification higher but also the risk that criminal proceedings become derailed due to procedural irregularities.[435] It is therefore crucial in such cases that full attention is given to the procedural requirements in the particular context in question.

7.2.2 Rules pertaining to electronic evidence

This section reviews the current legislation as well as the soon-to-be adopted new legal framework for electronic evidence in Europe. First, it examines frameworks coming from the Council of Europe and the European Union and then moves to examine the position of the national legislator within Europe, giving a brief overview of the legislation and practices applying to some states within Europe. Notably, although the EU provides a framework for adoption and guidance, the criminal law and the criminal procedural law, as also seen earlier in the discussion around cybercrime and cybersecurity, are a national matter. Moreover, it is also worthy to mention that as of now, there is no comprehensive international or European legal framework providing rules relating to evidence, in its traditional or electronic form.[436]

7.2.2.1 The Council of Europe´s framework

7.2.2.1.1 Current legislation

With regard to electronic evidence, a number of Council of Europe instruments and documents are highly relevant:[437]

- the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) in particular with reference to the protection of the rights to privacy and due process, as analysed in section 7.1;
- the Council of Europe Convention on Cybercrime, as this Convention remains the main and only international treaty which defines the substantive elements of cybercrimes, as seen in 6.1;[438]
- the Council of Europe Convention on Mutual Assistance in Criminal Matters, and its 1978 Protocol;[439]

[431] Biasiotti, M. et al [eds] (2018), Handling and Exchanging electronic evidence across Europe, Springer, p.191.
[432] Ibid.
[433] Ibid, p.192.
[434] Ibid, p.192.
[435] Quinn, P. (2016).
[436] Biasiotti, (2018), p.192.
[437] EVIDENCE project, European Informatics Data Exchange Framework for Courts and Evidence, D3.1 Overview of existing legal framework in the EU Member States.
[438] Ibid.
[439] Council of Europe, European Convention on Mutual Assistance in Criminal Matters, ETS No.030, Strasbourg 12 June 1962.

Copyright © Cyber-Trust Consortium. All rights reserved.

- the Electronic Evidence Guide.[440]

7.2.2.1.2 New proposed framework

In parallel with the EU legislative procedure that will be described in section 7.2.2.2.1, 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 following issues regarding electronic evidence.[441] However, the negotiations are not to be concluded before 2019.[442]

7.2.2.2 The EU framework

Judicial and police cooperation in European Union is subject to Art. 4 (2) of the Treaty on the European Union (TEU) which states that national security is the sole responsibility of each Member State. However, in accordance with Articles 82, 83 and 87 TFEU, the EU has adopted a number of Directives and other measures with regard to criminal law. In the following overview, only the relevant to electronic evidence instruments will be mentioned.

7.2.2.2.1 Current legislation

Currently, the following instruments are applied on matters relating to electronic evidence in EU:[443]

- The EU Charter of Freedoms and Rights: Law enforcement access to personal data, such as subscriber information, metadata (including traffic data, location data and access logs) and content data, constitutes an interference with the right to privacy, guaranteed under Article 7 of the Charter, and with the right to the protection of personal data, guaranteed under Article 8 of the Charter.[444] Under Article 52(1) of the Charter, any limitation 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. Limitations may be imposed on these rights and freedoms only if they are necessary and if they genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. Member States can impose limitations on the rights to data protection and to privacy, since it is provided for by EU law.
- Directives and Regulations that include general data protection principles, also applicable to electronic evidence: With respect to data processed by telecommunications and information society service providers, Article 23 of GDPR and Article 15 of Directive 2002/58/EC state to which extent limitations to data protection rights are acceptable. With respect to personal data processed by competent authorities for law enforcement purposes, Directive 2016/680, also provides for a specific data protection regime.[445] Chapter III of this instrument also permits the Member States 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 interests of the natural person concerned.

[440] Council of Europe, Data protection and Cybercrime Division, Electronic Evidence Guide, Strasbourg 3 February 2013.
[441] Council of Europe, Enhanced international cooperation on cybercrime and electronic evidence: Towards a Protocol to the Budapest Convention, 19 March 2018.
[442] 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.
[443] EVIDENCE project, European Informatics Data Exchange Framework for Courts and Evidence, D3.1 Overview of existing legal framework in the EU Member States.
[444] Statement of the Article 29 Working Party, Data protection and privacy aspects of cross-border access to electronic evidence, Brussels, 29 November 2017.
[445] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

- The European Investigation Order (EIO) Directive[446] sets up a new system that allows the EU Member States to obtain evidence from the other Member States in criminal cases that involve more than one Member States.
- The EU 2000 Convention on mutual assistance in criminal matters.
- 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.[447] The admissibility of files in electronic form as evidence was ensured in legal proceedings.
- The European Union Agency for Network and Information Security (ENISA) Handbook and Guide,[448] which outline a number of guiding principles for law enforcement authorities

The European Evidence Warrant (EEW) Decision was supposed to replace the system of mutual assistance in criminal matters among the Member States for the exchange of evidence for use in criminal proceedings (Art. 1 of EEW Decision) and established relevant procedures and safeguards. This is so far the only instrument which explicitly referred to electronic data as evidence. It lacked importance, however, because of its limited scope, applicable only to already existing evidence. In practice, competent authorities preferred the regime of Directive 2014/41/EU or mutual legal assistance procedures. Thus, the EEW was repealed by Regulation (EU) 2016/95 of the European Parliament and of the Council on 20 January 2016, regarding the repeal of certain acts in the field of police cooperation and judicial cooperation in criminal matters.[449]

7.2.2.2.2 New proposed legislation for cross-border transfer of evidence

Electronic evidence is needed in more than half of the criminal investigations and in almost all of them, the competent authorities have to request evidence from online service providers based in another jurisdiction.[450] Due to this extensive cross-border element, it seems that the Cyber-Trust prototype may have to consider such cases. The European Commission proposed on 17 April 2018 new rules in the form of a Regulation and a Directive, aiming to create a European Production Order, allowing 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 emergencies.[451] [452] It also aims to create a European Preservation Order, allowing a judicial authority in one Member State to request that a service provider or its legal representative in another Member State preserves specific before a production request is submitted and processed.[453] However, only stored data are covered by the proposal, whereas real-time interception of telecommunications is excluded.[454] Last but not least, service providers which offer services in EU but they are headquartered in a third country would have to designate a legal representative in the Union.[455]

[446] 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.
[447] The 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.
[448] 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.
[449] 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, p. 9–12.
[450] European Commission, Fact Sheet - Frequently Asked Questions: New EU rules to obtain electronic evidence, Brussels, 17 April 2018.
[451] Ibid.
[452] 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.
[453] European Commission, Fact Sheet - Frequently Asked Questions: New EU rules to obtain electronic evidence, Brussels, 17 April 2018.
[454] Ibid.
[455] Ibid.

Copyright © Cyber-Trust Consortium. All rights reserved.

7.2.2.3 At the Member States level

Only a few countries have modernised their legal systems to include technological developments. However, many still use outdated or old laws, implementing them on electronic evidence by analogy. Even though a unified European framework does not currently exist, there is a number of principles and good practices which seem to be shared by most jurisdictions.[456] According to ENISA´s guide on electronic evidence, there are five internationally accepted principles that are considered a good basic guideline for the collection and use of electronic evidence. These are a) data integrity, b) audit trail, c) specialist support, d) appropriate training and e) legality.[457] It is of paramount importance that anyone handling electronic evidence prior to their examination, treat it in such a manner that will give the best opportunity for any recovered data to be admissible as evidence in later proceedings.[458] Here are some examples of relevant legislation in the Member States:

i. Cyprus

In Cyprus, police authorities have the following investigative powers under national law: [459] search and seizure of information systems/computer data; preservation of computer data; order for stored traffic/content data; order for user information. Real-time interception/collection of traffic and content data is not allowed. There are no special admissibility rules related to electronic evidence, therefore, by analogy, it is subject to the same rules as conventional evidence and is admissible under the Evidence Law, Cap 9.[460] Electronic evidence is collected on the basis of international standards, and in line with the Police Order 3/17 and the Forensic Lab Manual.[461] The evidence, along with the investigator's report and the forensic examiner's report, is presented to the court and is available for use during the criminal proceedings.

ii. Greece

The Greek Code of Criminal Procedure covers the rules of evidence.[462] Regarding the means of proof, every lawfully acquired evidence is in principle admissible and can be adduced before Court, whereas investigating authorities and Courts as well have a duty to search for the factual truth (Articles 177, 351 and 357) being entitled to initiate any investigating act considered necessary to reveal the truth. The probative value of the various means of proof is in principle subject to the Court's free judgment. Art. 178 GCCP mentions the most common means of proof: indices, inspection of persons, places and objects, experts' reports, confessions, statements of witnesses and documents.[463]

iii. Italy

The collection and handling of electronic evidence is primarily covered by the Italian Code of Criminal Procedure, and in particular articles 244 et seq., 247 et seq. (searches), 248, 254bis, 259, 266 et seq. (telephone interceptions and electronic surveillance), 352, 354, 359, 360.[464] Article 244 regulates "digital inspection", establishing that the inspection of persons, places and objects occurs only if authorised and with

[456] Ingle, J. (2014); Jackson, J. and Summers, S. (2012).

[457] 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.

[458] Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, March 2012.

[459] 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.

[460] Ibid, p.39.

[461] Ibid, p.38.

[462] Quinn, P. (2016).

[463] 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].

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

Copyright © Cyber-Trust Consortium. All rights reserved.

the aim to ascertain the evidence of a crime.[465] The Law no. 48 of 18 March 2008 specified that, as far as electronic evidence is concerned in the provisions of the Code of Criminal Procedure, investigators shall adopt "the technical measures aimed at ensuring the preservation of original data and preventing it from being altered". The Italian Electronic Communications Code calls operators to assist judicial authorities by providing "compulsory services", which include delivery of data and interception of communication upon request.[466]

iv. Luxembourg

The Code of Criminal Procedure contains the rules on evidence. No specific admissibility conditions or restrictions apply to electronic evidence.[467]

v. The Netherlands

In the Netherlands,[468] 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 (Nederlandse Wetboek van Strafvordering (Sv)). For this requirement to be fulfilled, a judge must be convinced by the contents of legal evidence.[469] The evidence that the Dutch Code of Criminal Procedure considers admissible, concerns: the judge's own perception, statements by the accused, statements by a witness, statements by some expert, and other documents.[470]

The Cybercrime Law provides rules on the search of computer systems during a search of premises for the purpose of safeguarding computer data, including the extension of a search in connected systems and the order to decrypt or making inaccessible.[471] The powers for surveillance of electronic communications, as well as the legal order for the collection and disclosure of traffic data and subscriber data concerning electronic communications, are also covered in the Law, alongside with the expedited preservation of data, the expedited disclosure of traffic data and the interception of communications.[472]

In addition, the Dutch Code of Criminal Procedure regulates the use of certain powers in the investigation of serious crime,[473] in a section called the Special Investigative Powers Act, which entered into force in 2000, extending the means available for investigating organised crime by defining the ways the Dutch police can use covert methods, subject to the principles of proportionality and necessity. The powers concerned are: a. systematic observation; b. infiltration; c. pseudo purchases; d. systematic information gathering; e. sneak-and-peak operation; f. electronic interception of communications; and g. interception of private communications.[474]

In the first instance, a decision on whether a method is proportional is issued by the public prosecutor who has to check if the same results could be achieved by less intrusive means.[475] Her or his decision must be upheld by the investigative judge who will provide the actual authorisation to deploy the method in question.[476] In the case of "milder" special Investigative powers, such as retrieving historical data or traffic information, the investigative judge's consent is not necessary.[477]

[465] De Zan, T. and Autolitano, S. (2016), EUnited Against Crime: Improving Criminal Justice in European Union Cyberspace, Instituto Affari Internazionali. p.48.
[466] Ibid, p. 51.
[467] 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.
[468] Council of Europe, Status regarding Budapest Convention – The Netherlands, coe.int
[469] Borgers, M.J. and Stevens, L. (2010), The Use of Illegally Gathered Evidence in the Dutch Criminal Trial, Netherlands Comparative Law Association.
[470] Section 339 CCP.
[471] Odinot, G. et al. (2017), Organised Cybercrime in the Netherlands: Empirical findings and implications for law enforcement, Dutch Ministry of Justice.
[472] Council of Europe, Status regarding Budapest Convention – The Netherlands, coe.int
[473] Odinot, G. et al. (2017).
[474] Beijer et al. (2004), p. 277.
[475] Odinot, G. et al. (2017).
[476] Borgers, M.J. and Stevens, L. (2010).
[477] Odinot, G. et al. (2017).

Copyright © Cyber-Trust Consortium. All rights reserved.

vi. United Kingdom

In the United Kingdom, the law used by the law enforcement agencies to collect electronic evidence is the Police and Criminal Evidence Act 1984 (PACE). The two relevant clauses of PACE are Section 9(1) and Section 19(4).[478] Except for legislation, prosecutors refer as well to the ACPO guidelines.[479] Although a non-binding document, the Guide includes four important principles that law enforcement agencies must follow, when collecting and sharing electronic evidence, as follows: a. the data held on an exhibit must not be changed; b. any person accessing the exhibit must be competent to do so and explain the relevance and the implications of their actions; c. a record of all processes applied to an exhibit should be kept; d. this record must be repeatable to an independent third party. The person in charge of the investigation has responsibility for ensuring the legality of the procedure.

7.3 Use of Blockchain for the storage of electronic evidence

7.3.1 State of play

Electronic evidence plays an essential role in cybercrime investigation, and thus technical measures that can guarantee integrity, authenticity, and auditability of evidentiary material, as it moves along different levels of hierarchy in the chain of custody during the criminal proceedings is of high relevance. The Cyber-Trust project aims to utilise blockchain technology's capability of enabling a comprehensive view of transactions back to origination in order to store safely electronic evidence.[480]

There seems to be a tendency worldwide in the police and security sector to centralise the collection of evidence and case files. The disadvantage of a centralised system is that, by its structure, it can be more vulnerable towards attacks and thus, requires a very high degree of security.[481] Law enforcement needs a system that is above all secure, and that can control information sharing effectively. Blockchain or in general, Distributed Ledger Technologies (DLTs) could contribute, ensuring that no single party can control the system, reducing this way the risk of manipulation. UK, Australia and China already experiment with such systems in the police and justice sector. Nevertheless, the practice is far from common, and there is no case law to draw conclusions from yet.

Blockchains are different from the standard conception of a traditional database and thus, raise serious challenges under data protection law.[482] The key distinction between permissioned and unpermissioned blockchains is access rights, in other words who can participate, read and write. In addition to public and private blockchains, hybrids have also emerged, such as the consortium blockchains and their variations, which are partially decentralised. Concerning the Cyber-Trust project, two questions are of high importance and have to be examined: first, do data related to a natural person stored on a decentralised ledger qualify as personal data in EU law? And second, can data stored in such a manner, carrying or not personal information, be admissible during criminal proceedings in various jurisdictions? A more detailed overview of those issues, briefly touched upon here, will be offered in D3.2.

7.3.2 Blockchain and data protection issues

Legal scholars and technologists are currently trying to determine whether they can legally store and process personal data on ledgers in EU. The answer to this question is highly dependent upon whether such activity

[478] 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.

[479] Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, March 2012.

[480] Blockchain is an application, while Distributed Ledger Technologies (DLT) are the underlying technology. Since Blockchain was the first successful implementation of a DLT system, oftentimes the two terms are used interchangeably. In the forthcoming deliverable D3.2, we will provide the reader with an in-depth analysis on the topic. There, we will give preference to the term DLT, in order to make sure that irrespective of the final technical solution the Cyber-trust consortium will choose, our findings will still be applicable. In this first deliverable, for reasons of simplicity, we will use the term Blockchain.

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

[482] Filippone, R. Blockchain and individuals' control over personal data in European data protection law, Tilburg University, August 2017, p.16.

Copyright © Cyber-Trust Consortium. All rights reserved.

falls within the scope of the EU's data protection regime or not. The GDPR, as the central piece of EU legislation concerning data protection, is most relevant to a centralised perception of the collection, storage and processing of data and less to a decentralised one. Blockchains, on the other hand, offer decentralised handling of data, which provides a form of data sovereignty and authenticity. For data sovereignty objectives to be achieved, they must be combined with additional mechanisms, because if not adequately safeguarded, blockchains could expose all data stored in them.[483] Depending on the respective Blockchain´s 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. by hashing them to the chain.[484]

Data stored on a blockchain in plain text are still personal data under GDPR, because they can identify an individual.[485] Encrypted data are also personal data since they can still be accessed with the correct keys and thus, encryption does not make the data irreversible unidentifiable, as required by GDPR in order to be regarded as anonymised.[486] Lastly, personal data which have been processed through a hashing function, also seem to be regarded as personal data under GDPR.[487] Although a hash process offers stronger guarantees than encryption, the Article 29 Data Protection Working Party has stated that hashes constitute pseudonymised data and not anonymised, since they could still be linked to an individual.[488]

However, even though techniques being used at the moment for storing personal data on a blockchain seem not to be out of the scope of GDPR, this might not always be the case in the near future.[489] Both of the following ideas are of relevance for Cyber-Trust and will be subject of further elaboration in the next two deliverables D3.2 and D3.3. First, since the use of blockchain becomes more and more common, there will be cases where courts or the EDPB will be called to decide upon whether some cryptographic processes can be considered capable of anonymisation or at least, offer protection equal to anonymisation.[490] Such a decision would 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 more tools based on specifications, legally recognised as anonymisation techniques.

Second, technical solutions are currently being developed in order to achieve GDPR compliance, that may result in a sustainable combination of off-chain and on-chain mechanisms.[491] For instance, personal data could be stored in an off-chain conventional database 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 availability and security of the off-chain database. In addition, metadata should also be treated appropriately as they could reveal personal information even where personal data are not directly stored on-chain.

Another issue that arises is whether a user's public key constitutes personal data or anonymous data.[492] A public key seems to fall into the pseudonymisation scope, meaning that it "can no longer be attributed to a specific data subject",[493] however, if combined with "additional information", it could potentially result in the identification of a user.[494] The biggest challenge about public keys is that they cannot be moved off-chain and thus, GDPR-compliant solutions are more difficult to identify[495]. Some instances constitute the use of a

[483] 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.
[484] Finck, M. (2018), Blockchains and Data Protection in the European Union, European Data Protection Law Review, 4 (1), pp. 17 – 35.
[485] Ibid, p.22.
[486] Ibid, p.22.
[487] Ibid, p.23.
[488] Ibid, p.25.
[489] Ibid.
[490] Ibid.
[491] Ibid.
[492] Ibid, p.24.
[493] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014, 0829/14/EN WP216, p.12.
[494] Finck, M. (2018), p.24.
[495] Ibid, p.25.

Copyright © Cyber-Trust Consortium. All rights reserved.

stealth address, which relies on hashed one-time keys, or processes that only reveal whether a transaction has occurred, or the use of state channels for two-side smart contracts that only share information with outside parties in the event of a dispute, or adding "noise" to the data.[496] [497]The Article 29 Data Protection Working Party confirmed that, provided that the necessary safeguards are complied with, the addition of noise may be an acceptable anonymisation technique in combination with "the removal of obvious attributes and quasi-identifiers".[498]

Where there is processing of personal data in the blockchain, enforcing individuals´ rights, under those circumstances, would also pose a number of challenges. One issue is the identification of the data controllers. For instance, in particular in public blockchains, it might be impossible to identify a central operator.[499] Equally difficult would be to determine the exact number, location and identity of nodes, especially, on a public blockchain, if it was accepted that each node qualifies as a separate data controller.[500]

Since nodes may be located in various jurisdictions across the globe,[501] the GDPR's extended territorial scope will subsequently cover activities with only an indirect link to the EU.[502] A jurisdictional question that pops up relates to the application of European data protection requirements to the transfer of data to third countries.[503] 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 if a number of specific conditions is satisfied. Compliance with this provision would be almost impossible in a blockchain context, for the data stored in blocks are hashed to the chain by miners that can be based anywhere in the world, even in states or organisations which do not offer an adequate level of data protection.[504] Thus, it is imperative for the partners to take into consideration all these issues before choosing the type of blockchain and its particular characteristics.

7.3.3 Blockchain and admissibility of evidence in criminal proceedings

In criminal proceedings, blockchain technology has the potential to be used to keep track of the chain of custody once evidence is obtained and taken later for analysis. Using blockchain to store and to standardise all this data could offer the same security level as a paper trail but with less hassle. This is particularly true when it comes to electronic evidence, such as browser records or digital documents or the wide range of devices which may contain electronic evidence.[505] The abundance of electronic products, devices and services pose challenges to the evidence examiner, since there is no uniform process to obtain this crucial information.[506] Extraction is a rather complicated and sophisticated procedure, which could mean interference with the privacy of both suspects and victims as well as other data subjects, as all involved parties may have their own personal devices and are somehow related to the investigation.

Storing evidence in the blockchain would include the generation of a digital fingerprint, known as "hash", unique to each digital object and sensitive to even the smallest alterations. As soon as a digital object is accepted into evidence, the digital fingerprint is passed into a blockchain, public or private. The digital footprint, automatically, receives the following features:[507] First of all, it is given a degree of immutability.

[496] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014, 0829/14/EN WP216, p.12.
[497] Finck, M. (2018), p.25.
[498] Ibid.
[499] Ibid: "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'."
[500] Ibid.
[501] Ibid.
[502] Ibid, p.27.
[503] Ibid.
[504] Ibid, p.28.
[505] Rands, K., How blockchain is disrupting the legal industry, Global Legal Blockchain Consortium, 9 June 2018.
[506] Goodison, S. E et al (2015), Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. Santa Monica, CA: RAND Corporation.
[507] Based on the unofficial report issued by the UK government, see: Davidson, A., Increasing trust in criminal evidence with blockchains, 2 November 2017, gov.uk

Copyright © Cyber-Trust Consortium. All rights reserved.

This means, once written, the digital fingerprint is permanent and cannot be removed, even by the writer themselves, unless under specific circumstances. Second, every block in a public blockchain is timestamped in a way that is impossible to forge.[508]
Third, every full node in the blockchain network has a complete copy of the distributed ledger, leading to availability and accessibility at all times.[509] Fourth, the digital footprint carries a high degree of transparency guarantees, since depending on the access rights, anything written to blockchain is readable by anyone in the world or by a member of a specific group, ensuring integrity and validity. This leads to the fifth feature, i.e. the distributed trust, which minimises administrative problems and simplifies the "chain of custody" process.
If the aforementioned features are guaranteed and if the collection of evidence has followed the legal requirements and principles, described in section 7.2.2, the storage of evidence in blockchain seems to follow most of the principles described in ENISA´s guide on electronic evidence, for instance, data integrity and audit trail.[510] However, admissibility 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. What is left is to wait for the case law and see how each jurisdiction will decide upon the admissibility of such evidence in the future.

[508] Blockchain technologies have yet to tackle some technical challenges in order to be considered an effective forensic evidence storage tool. For instance, by recording a digital fingerprint, what is certified is that at a given moment, this digital asset existed in precisely this form and that a specific organisation added it. However, it cannot be proven that the digital asset has never been tampered with or falsified before its entry on the blockchain.
[509] Davidson, A. (2017).
[510] 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.

Copyright © Cyber-Trust Consortium. All rights reserved.

8. Conclusions

8.1 Overview of implications related to Cyber-Trust and recommendations

8.1.1 Privacy

The proposed Cyber-Trust prototype represents a technology that will be used for cyberthreat intelligence gathering and sharing purposes, with the aim to contribute to information and network security, while eliminating the number of cyberthreats and cyberattacks. As such, the Cyber-Trust prototype will use monitoring and filtering techniques, which could amount to digital surveillance with the potential to affect the privacy of individuals. The notion of **informational privacy** seems to fit best in the context of Cyber-Trust. However, a recognition of the harms that digital surveillance practices can entail for **privacy in the broad sense**, is also important, since the expected use of the Cyber-Trust prototype may involve monitoring of communications in public fora in the darknet and the clearnet as well as the use of publicly available blacklisted IP addresses and deep packet inspection techniques leading to the profiling of specific IoT devices for cyber-threat intelligence and attack detection and mitigation purposes. This is because individuals may not want to be monitored, even if in a public forum, or even if personal information that can be specifically connected to them as individuals is not recorded.

Privacy is protected in a considerable number of international and European legal instruments. Two of the most prominent provisions are **Article 7 of the European Union's Charter of the Fundamental Rights (CFR)** which explicitly recognises a fundamental right to privacy under the notion of "respect for private and family life, home and communications", and the **Article 8 of the European Convention on Human Rights (ECHR)**, which has been applied in several cases related both to the narrow "informational" concept of privacy as well as the broader notion of privacy, and is of more direct importance for Cyber-Trust.

As elaborated in the case law of the European Court of Human Rights (ECtHR), intrusions in privacy may not necessarily constitute privacy violations, since a **case-by-case assessment** should consider the **competing values in question, i.e. privacy and security**. For instance, when a tool is used to detect, prevent or mitigate large-scale cyberattacks which could pose a serious risk for the safe operation of critical infrastructure, harms to personal privacy allegedly experienced by some individuals may be not sufficient to render the aims behind the security measures, disproportionate. For **a right to privacy is not absolute**, if the state did not act in order to protect the critical infrastructure and consequently human life, it would arguably not be meeting its obligations towards its citizens of providing security and protecting life and property.

This does not mean that by the mere fact that where the Cyber-Trust prototype is used in order to detect, prevent or mitigate crime, its usage will automatically be considered legal. **An assessment should be made in the particular context, in order to figure whether the conditions of proportionality and necessity are met and whether the usage of the tool is compliant with the specific national law in each case**. The notion of proportionality and the respective proportionality test, as suggested in the case law of the European Court of Human Rights (ECtHR), provide a way of judging when such interferences with privacy may be acceptable or not.

Internet research ethics as well as computer ethics, as part of general research ethics, could form a point of reference for areas which are still underdefined in law, during the research phase of the project**.** The incomprehensive public/private distinction in the virtual environment, suggests that researchers must define the legal framework and social norms that apply on an online or networked space before making assumptions about the "publicness" of information shared within.

8.1.2 Data Protection

With respect to Cyber-Trust, the two leading EU legislative initiatives, that are likely to be relevant to the project are **the General Data Protection Regulation (GDPR) and the Directive 2016/680 (Police Directive)**. During the research phase, the GDPR will be applied to the research activities whenever personal data are being processed, whereas after the launch of the prototype, its potential use by law enforcement agencies for the detection, prevention and prosecution of malicious activity may be exempted from the field of application of the Regulation 2016/679 by Recital 19 which excludes its application to personal data being used in connection to police and criminal justice activities on grounds of public safety, public security, and

Copyright © Cyber-Trust Consortium. All rights reserved.

public order. In that case, such processing may fall under the scope of Directive (EU) 2016/680 and the respective national law.

Of certain significance may also be the **e-Privacy Directive** (and the upcoming e-Privacy Regulation), concerning the confidentiality of communications. The **invalid Data Retention Directive** may also be relevant insofar as its provisions remain valid in the different Member States, where the implementing legislation was not withdrawn or updated after the invalidation of the Directive by the Court of Justice of the European Union. It is highlighted that **the data protection principles create a system of checks and balances, which can be engaged even where there is no demonstrable harm to individual privacy**, as seen above. This is important for the Cyber-Trust partners who may process personal data, as it means that breaches of data protection principles and rules can occur even where no individual has complained of harms to his or her privacy because such infringement is not necessary for data protection rules to be triggered.

Since the Cyber-Trust project will deploy cyberthreat intelligence techniques engaging a vast amount of data from internal, community and external sources, it is likely that there will be moments when questions will arise as to whether particular data are personal or not. It is important to mention that a **case-by-case assessment should take place, in order to conclude whether the data are personal in the specific context**. In general, in order to determine whether the data could lead to the identification of an individual, partners may need to consider:[511] the content of the data; the purpose of the processing; and the results of or effects on the individual from processing the data.

"Online identifiers", for instance, include IP addresses and cookie identifiers which could be regarded as personal data. However, other attributes may also lead to the identification of an individual, such as aggregate network indicators and network flow data. This implies that a combination of identifiers may be adequate to identify an individual indirectly, and hence, this information may constitute personal data, even if additional information is required in order to be able to actually proceed with the identification of an individual. That additional information could be already at someone´s disposal or must be collected from another source. Even if data does not relate to an identifiable individual in the hands of one controller, it may do in the hands of another. In order to assess whether individuals are identifiable based on this data, all the means that could be used "by an interested and sufficiently determined person", must be taken into consideration. The partners are also under the obligation to control whether the chances for identification have increased or diminished over time, for instance due to developments in technology and science.

Even after all those assessments, there will perhaps still be circumstances where it may be difficult to determine whether data are personal or not. **If in doubt, as a matter of good practice, the information should always be treated with the necessary care, by ensuring that a lawful basis for processing does exist and in particular, all necessary technological and organisational measures and security safeguards are in place.** If partners use anonymisation techniques, then the **anonymised data are not subject to the GDPR**. Pseudonymisation measures can help reduce privacy risks and may constitute an appropriate safeguard under specific circumstances, however, **pseudonymised data are still personal data and should be treated as such.**

When personal data are processed – even for the time until its anonymisation, such **processing must always have a legal basis, either laid out in the GDPR (during and after the project) and/or in the Directive 2016/680 (after the end of the project), as transposed in the national legislations.** The legal bases may also be found in other relevant legal instruments, for instance domestic laws about data interception and retention. Under GDPR, during the research phase the sole legal base is the consent of the data subjects (Article 6(1)(a) GDPR), whereas after the research phase, the most relevant legal grounds seem to be the consent of the data subjects and the existence of a legitimate interest (Article 6(1)(f) GDPR).

When the processing falls under the scope of Directive 2016/680, it is lawful only if and to the extent that it is necessary for the performance of a task carried out by a competent authority for the purpose 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 that is based on Union or Member State law. **Consent of the data subject can never in itself constitute a legal**

[511] In general, the Information Commissioner´s Officer´s website offers detailed guidance and checklists, when issues arise in relation to personal data definitions.

Copyright © Cyber-Trust Consortium. All rights reserved.

ground for the processing of data in the context of the Directive. Where the data subject is required to comply with a legal obligation, it should be understood that the data subject has no genuine and free choice. **The roles of the research partners in the data processing should be clarified.** Data controllers in the project are required to register with their national supervisory authorities, wherever necessary and appoint a Data Protection Officer to assist them with their compliance duties throughout the project. In preparation of the Data Protection Impact Assessment that will be conducted in D3.4, whenever partners have to deal with personal data processing, should be able to provide a systematic description of the processing; to demonstrate that the nature, scope, context and purposes of the processing have been taken into account; to keep record of the specific personal data, recipients and period for which the personal data are stored; to identify the assets on which personal data rely (hardware, software, networks, etc); and to take into account approved codes of conduct, if any.

Moreover, **in all stages of the project data controllers must assess necessity and proportionality of processing, by determining the specific measures envisaged to comply with the GDPR principles:** demonstrating a specified, explicit and legitimate purpose and guaranteeing lawfulness, fairness and transparency of processing, data minimisation and accuracy, limited storage duration, data security and accountability. Without prejudice to exemptions applied in the specific context of each case, **the data controllers must also take all necessary measures to safeguard the rights of the data subjects**, by ensuring that the rights to information (Articles 12, 13 and 14 GDPR) and access (Articles 15 GDPR), rectification and erasure (Articles 16, 17 and 19 GDPR) as well as the rights to object and restrict the processing (Article 18, 19 and 21 GDPR) are properly communicated to the data subjects, and can be fully enforced. If personal data are to be transferred to a third country outside the EU, the data controller must make sure that all safeguards surrounding international transfers are provided (Chapter V GDPR).

The Cyber-Trust as a research project should implement the notions of data protection by design and by default, as introduced in the GDPR. Doing so, for instance, by designing the tool in a manner that is able to detect and record activity that is highly likely to be of criminal nature, the chances are higher that the use of the tool in a particular circumstance will be deemed as being proportional. A failure to engage privacy enhancement tools could have as a result that the Cyber-Trust prototype would be used only in the gravest of contexts and would reduce both its appeal and potential uptake.

If risks to the rights and freedoms of data subjects are identified, they should be managed promptly, and the origin, nature, likelihood, particularity and severity of the risks should be determined, in particular in relation to incidents of illegitimate access, undesired modification, or disappearance of data. The data controllers should take into account the potential impact of those risks to the rights and freedoms of the data subjects and have in place sufficient countermeasures to mitigate them. Whenever sufficient measures to reduce the risks to an acceptable level cannot be identified, consultation with the supervisory authority is required. **Pseudonymisation, encryption as well as data minimisation, oversight mechanisms, etc. are only indicative examples of appropriate measures, which means that they are not "by nature" appropriate. The implementation of appropriate measures depends on the context and the risks, specific to each processing operation.**[512]

8.1.3 Cybercrime and cybersecurity

The regulatory framework regarding cybersecurity and cybercrime is relevant for the Cyber-Trust project with regards to its end-users and the potential launch of the tool. The Council of Europe **Convention on Cybercrime** as well as the **EU Directives 2013/40 on attacks against information systems and 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)** in conjunction with the relevant implementing Regulation 2018/151, are the legal instruments of higher importance for the project. In order for Cyber-Trust partners to achieve an effective design, it will have to **determine early its area of action**, in other words the types of cybercrimes that it will try to detect and mitigate, taking into account what is accepted as cybercrime in the different jurisdictions

[512] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, adopted on 4 April 2017, 17/EN WP 248 rev.01, p.19-21.

Copyright © Cyber-Trust Consortium. All rights reserved.

where the system will be deployed as well as its end-users and the exact purposes of its use (for instance, for law enforcement purposes). It is underlined that not all types of what is commonly accepted as "cybercrime" in non-legalese are legally prosecuted.

National legislations were adopted the last years based on the obligations introduced by the legal instruments mentioned above. Since all these instruments require acts from the side of the Member States in order to be fully transposed into national law and at the same time permit States to opt for derogations regarding specific provisions, the European legal framework is not harmonised. Nevertheless, **most of the examined states seem to follow or intend to adopt similar approaches and their domestic laws cover to an extent and with only few exceptions all the criminal offences identified in the EU law**, namely: a. illegal access to information systems; b. illegal system interference (by inputting computer data, transmitting, damaging, deleting, deteriorating, altering or suppressing such data, rendering it inaccessible which could result in seriously hindering or interrupting the functioning of an information system); c. illegal data interference; d. illegal interception of non-public transmissions of computer data and electromagnetic emissions from an information system carrying such data e. illegal provision of tools used for committing the aforementioned offences; f. incitement, aiding and abetting by natural and/or legal persons to commit all the aforementioned offences as well as attempt to commit offences covered under b and c. Therefore, the Directive 2013/40 criminalises the use of malicious software, such as "viruses" and "botnets", or of unlawfully obtained computer passwords, while includes the obligation of the Member States to collect basic statistical data on cybercrime.

The same observations, as above, apply to the implementation of the NIS Directive in national law; however, **the transposition of the NIS Directive is still pending in many EU Member States**, including Greece, The Netherlands and Luxembourg. As a first step though, most states have already adopted National Cybersecurity Strategies, which constitutes one of the requirements of the NIS Directive.

Some indicative recommendations, with regards to cyberthreat intelligence tools, envisaged to be used or created by the Cyber-Trust project for the prevention, detection and mitigation of cybercrimes: **A platform that includes information on threats** that could allegedly deploy malicious attacks or are related to alleged malicious activity, including profiled or blacklisted devices or IP addresses, created for the Cyber-Trust purposes **needs to be kept up-to-date and accurate**, to as great an extent as possible. As there will always be a margin of false alerts, **a balancing exercise is needed to weigh up the risks of using the data on this platform** for further cyberthreat intelligence purposes. **Profiling techniques based on the use of automated tools carry potential risks,** not only because individuals might not expect their personal information to be used in such a way and might not understand how such processes work, but also because **decisions taken may lead to significant adverse effects**, for instance, the application of increased security measures or surveillance by competent authorities. Even where national laws provide exceptions, **suitable safeguards must be put in place for the rights and freedoms of data subjects,** including the right to obtain human intervention, in particular, to express his or her point of view, to obtain an explanation of the decision or to challenge it.

Moreover, since cyberthreat intelligence information is going to be collected from various sources, **the partners should make sure that personal data that may be found during the searches are obtained by lawful means by the organisation that provided the data to the specific website, on an appropriate legal ground (such as consent, legal obligation, or public task of the controller) and that the data shared via the portal or website are proportionate.** A case-by-case analysis is particularly important regarding web crawling for data "available in the public domain", since harvesting data via web-crawlers, for example, may raise questions of purpose limitation as well as accuracy of a database populated in such a manner. **Although there is no specific law against scraping or using publicly available information which has been obtained through the use of scraping tools, an assessment of whether there is an infringement or not has to take place on a case-by-case level**; questions to be asked are to what extent is the data the result of creative input and therefore protected by copyright; or what amount of data are being scraped, and is the re-use prohibited in the terms and conditions of the website or the website requires specific access rights.

Inspection techniques based on IP headers and in particular, those based on deep packet inspection involve the monitoring and filtering of a vast amount of data and may have severe implications in terms of privacy and data protection, as well as confidentiality of communications. The implications might be broader since,

Copyright © Cyber-Trust Consortium. All rights reserved.

depending on the effects pursued with the monitoring and interception, it is not the same to merely inspect communications, for example, to ensure the proper function of a system, and to inspect communications to apply policies which may have an impact on individuals, for instance for law enforcement purposes. The correct application of monitoring, inspection and filtering techniques must be conducted in compliance with the applicable data protection and privacy safeguards, which lay down limits as to what can be done and under which circumstances. **Under data protection legislation, the processing of personal data, such as in this case the processing of traffic and communication data, requires an adequate legal ground.** Specific requirements may apply in certain cases, depending on the type of personal data that are processed.

8.1.4 Electronic evidence

One non-legal definition of electronic evidence reads, as follows: "any information of potential probative value that is manipulated, generated through, stored on or communicated by any electronic device". The Cyber-Trust prototype, with the use of cyberthreat intelligence tools, aims to collect forensic evidence, admissible in EU courts, that links cybercriminals to specific threats and incidents. **Since the rules and principles governing the admissibility of evidence are to be found in the national codes of criminal law and criminal procedure, the Cyber-Trust partners will have to consider the regulatory framework of every jurisdiction where the evidence is to be submitted.** Nevertheless, both at European Union and Council of Europe level, **there is at the moment a legislative effort to harmonise the regulatory frameworks with regards to evidentiary law**, including electronic evidence. At Member State level, only a few countries have modernised their legal systems to include technological developments. However, the majority still uses outdated or old laws, implementing them on electronic evidence by analogy.

Given the nature of electronic evidence, risks are higher with regards to the fair management and presentation of evidence, including falsifying, destroying and manipulation of evidence. Furthermore, the complexity of electronic evidence means that is not only the risk of falsification greater but also the risk that criminal proceedings become derailed or halted because of procedural irregularities. It is therefore significant in such cases that great attention is given to the procedural requirements in place in the particular context in question. **There is a number of implicit general principles which the European Court of Human Rights has recognised to apply on the collection and use of evidence in criminal proceedings,** contributing to the interpretation of the relevant domestic law: **a. fairness of the proceedings** as a whole, implying that any evidence has been collected in a lawful way and without violating the rights and freedoms of the defendant, irrespective of whether the evidence holds truth; **b. quality of the evidentiary material,** in other words, reliability or accuracy of evidence; **c. appropriate oversight of surveillance activities** by competent monitoring authorities be it a judge or a prosecutor; **d. special investigation methods should not incite criminal activity.**

Moreover, 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. **According to ENISA´s guide on electronic evidence from 2014, there are five internationally accepted principles** that are considered a good basic guideline for the collection and use of electronic evidence. These are related to: **a. data integrity** (documentation of the chain of custody is crucial for ensuring the authenticity of the evidentiary material, in particular, if alterations were unavoidable), **b. audit trail** (chain of evidence, for the preservation of integrity), **c. specialist support** (forensics experts should seek assistance from specialists, if necessary, to ensure the right handling of evidence) **d. appropriate and constant training** and **e. legality** (seeking proper legal guidance, depending on the jurisdiction). It is of paramount importance that anyone handling electronic evidence prior to their examination, treat it in such a manner that will give the best opportunity for recovered evidentiary data to be admissible in later proceedings.

As for the storage of the evidence material in a blockchain application, **the partners should consider whether they will make use of a public, private or hybrid blockchain solution**. Depending on this choice, there will be different legal implications, for instance with regards to identifying the data controllers, and jurisdictional questions, in particular in the case of permissionless blockchains. **The partners should, moreover, take into account that as long as personal data are stored in the blockchain (irrelevant of which form they have: plain text, encrypted text, hashes, or public keys), the GDPR may apply, since pseudonymised data are still personal data. Data protection enhancing solutions should be explored**, for example, concerning whether

Copyright © Cyber-Trust Consortium. All rights reserved.

personal data could be stored off-chain and linked to the blockchain through a hash pointer; metadata should also be treated promptly as it could reveal personal information even where personal data are not directly stored on-chain. Unlike other personal data, public keys cannot be moved off-chain. Thus other GDPR-compliant solutions should be considered. As for the admissibility of electronic evidence stored in blockchain, **the features of a blockchain solution, seem in principle, to support ENISA´s abovementioned principles concerning storage and chain of custody,** however, it is highlighted that **relevant case law is yet to be formed and specific guidance from competent authorities to be given**, providing more certainty and a degree of standardisation in the field.

8.2 Final remarks

This deliverable provided in broad terms an initial examination of the legal and ethical principles relevant to the Cyber-Trust project. It is important to stress that this is not a contextual analysis of the legal issues triggered by the Cyber-Trust system, which will be subject of the upcoming deliverables, but rather a broader, holistic discussion of the relevant frameworks that should be taken into consideration throughout the project.

Part A of the deliverable began with an examination of the ethical aspects of the project, particularly the need to measure the importance of privacy against the equally important value of cybersecurity, given the subject matter of this project. Part B described the data protection regime potentially applicable to Cyber-Trust, whereas Part C offered a more detailed insight into the legal frameworks relevant to the regulation of cybercrime and cybersecurity in Europe. Part D provided an initial look at the legal regime of electronic (or digital) evidence in Europe.

By outlining the key legislative requirements that are likely to apply to the Cyber-Trust project, the main aim of this deliverable was to provide input for tasks T5.1 and T6.1 on cyber-threat intelligence information gathering and privacy-preserving device profiling respectively. These tasks will be necessarily restrained based on what is legally and ethically permissible. Appropriate practices and technical measures will be implemented with regards to data collection from various sources, that will meet all legal requirements pertaining to the use of personal data.

The Deliverable D3.1 will be the basis for D3.2 concerning the legal analysis of the use of evidence material, D3.3 concerning concrete recommendations for the design of the Cyber-Trust platform and its other tools and D3.4 – the first data protection impact assessment carried out during the design phase of the project.

Copyright © Cyber-Trust Consortium. All rights reserved.

References

Literature

Abdelgawad, E.L. (2009), The Execution of the Judgments of the European Court of Human Rights: Towards a Non-coercive and Participatory Model of Accountability, ZaöRV 69 (2009), 471-506.
Acquisti, A. and Gross, R. (2006), Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, Proceedings of the 6th Workshop on Privacy Enhancing Technologies, 4258: pp. 36–58.
Banisar, D. and Davies, S. (1999), Global trends in privacy protection: An international survey of privacy, data protection and surveillance laws and developments, in: John Marshall Journal of Information and Technology and Privacy Law, Vol.18(1).
Bennett, C. J. (1992), Regulating Privacy: Data Protection and Public Policy in Europe and the United States (Ithaca: Cornell University press).
Besson, S. (2015). The bearers of human rights´ duties and responsibilities for human rights: a quiet (r)evolution? Social Philosophy and Policy, 32(1), 244-268.
Biasiotti, M. et al [eds] (2018), Handling and Exchanging electronic evidence across Europe, Springer, p.191.
Bloustein, E. (1984), Privacy as an aspect of human dignity: An answer to Dean Prosser. In F. Schoeman (Ed.), Philosophical Dimensions of Privacy: An Anthology (pp. 156-202). Cambridge: Cambridge University Press.
Brants, C. & Franken, S., (2009). The protection of fundamental human rights in criminal process, General report. Utrecht Law Review. 5(2), pp.7–65.
Buchanan, E. A. and Zimmer, M. (2018), Internet Research Ethics, The Stanford Encyclopaedia of Philosophy (Spring 2018 Edition), Edward N. Zalta (ed.).
Bygrave, L. (1998), Data Protection pursuant to the Right to Privacy in Human Rights Treaties," International Journal of Law and Information Technology Vol.6(3), pp. 247–284.
C. Landwehr et al. (2012), Privacy and Cybersecurity: The Next 100 Years, in Proceedings of the IEEE, vol. 100, no. Special Centennial Issue, pp. 1659-1673.
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.
Cavoukian, A. (2011), Privacy by Design: The 7 Foundational Principles, Information & Privacy Commissioner, Ontario, Canada.
Cohen, J. (2013), What Privacy is for, Harvard Law Review 126(7), 1904-1933.
de Hert, P. and Gutwirth, S. (2009), Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalization in Action, in: Gutwirth, S., Poullet, Y., de Hert, P., de Terwangne, C., Nouwt, S. (Eds.), Reinventing Data Protection, Springer Netherlands.
De Zan, T. and Autolitano, S. (2016), EUnited Against Crime: Improving Criminal Justice in European Union Cyberspace, Instituto Affari Internazionali. p.48.
EVIDENCE project, European Informatics Data Exchange Framework for Courts and Evidence, D3.1 Overview of existing legal framework in the EU Member States.
Fabbrini, F. (2015), Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S, in: Harvard Human Rights Journal 28, Tilburg Law School Research Paper No. 15/2014.
Fantin, S. (2018), Law enforcement and personal data processing in Italy: implementation of the Police Directive and the new data retention law, DANTE project, kuleuven.be
Finck, M. (2018), Blockchains and Data Protection in the European Union, European Data Protection Law Review, 4 (1), pp. 17 – 35.
Fried, C. (1968), Privacy, in: Yale Law Journal Vol.77, p.483.
Friedewald, M. (Ed.), Burgess, J. (Ed.), Čas, J. (Ed.), Bellanova, R. (Ed.), Peissl, W. (Ed.). (2017). Surveillance, Privacy and Security. London: Routledge.
Georgieva, I. (2015), The Right to Privacy under fire – Foreign surveillance under the NSA and the GCHQ and its compatibility with Art. 17 ICCPR and Art. 8 ECHR, in: Utrecht Journal of International and European Law, Vol.31(80).

Copyright © Cyber-Trust Consortium. All rights reserved.

Gercke, M. (2012), ITU publication - Understanding cybercrime: phenomena, challenges and legal response, Telecommunications Development Sector.
González Fuster, G., (2014), The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer International Publishing.
Goodison, S. E et al (2015), Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. Santa Monica, CA: RAND Corporation.
Greenleaf, G. (2014), Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories in: Journal of Law, Information & Science 23(1), Special Edition: Privacy in the Social Networking World.; UNSW Law Research Paper No. 2013-40.
Guastamacchia, F. (2017), The role of blockchain in revolutionizing and re-organizing security: Evidence and policy recommendations, LUISS Universita Guido Galli, p.51.
Ibarra-Esquer, J.E. et al (2017), Tracking the Evolution of the Internet of Things Concept Across Different Application Domains, in Sensors.
Ingle, J. (2014), Overview: Criminal Law, Evidence and Procedure, Cambridge Journal of International and Comparative Law 3, pp. 265-268.
Jackson, J. and Summers, S, (2012), The Internationalisation of Criminal Evidence.
Joseph, S, Schultz, J. & Castan, M. (2004), The International Covenant on Civil and Political Rights: Cases, Materials and Commentary, Oxford University Press.
Koffeman, N.R. (2010), (The right to) personal autonomy in the case law of the European Court of Human Rights, Leiden.
Kokott, J. and Sobotta, C. (2013), The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR, in: International Data Privacy Law Vol.3 (4), pp.222–228.
Kuner, C. (2007), European Data Protection Law: Corporate Compliance and Regulation, Second Edition, OUP UK.
Kuner, C., The European Union and the Search for an International Data Protection Framework, in: Groningen Journal of International Law, vol.2, ed.1: Privacy in International Law.
Lango, J. (2006), Last Resort and Coercive Threats: Relating a Just War Principle to a Military Practice. Joint Services Conference on Professional Ethics.
Loideain, N.N. (2015), EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era in: Media and Communication, 2015, Volume 3, Issue 2, pp. 53-62.
Lynskey, O. (2014), Deconstructing data protection: the added-value of a right to data protection in the EU legal order in International and Comparative Law Quarterly Vol.63, pp 569-597.
Maglaras, L. et al. (2018), NIS directive: The case of Greece in Security and Safety.
Mai, J-E. (2016), Big data privacy: The datafication of personal information, The Information Society, 32, 3, (192).
Marx, G.T. (1998), An Ethics For The New Surveillance, The Information Society, 14 (3).
McCrudden, C. (2008), Human Dignity and Judicial Interpretation of Human Rights, in: European Journal of International Law Vol.19(4), pp. 655–724.
Miller, A. R. (1971), The assault on privacy: Computers, data banks, and dossiers. Ann Arbor: University of Michigan Press.
Milne, G. R. and Culnan, M.J. (2004), Strategies for Reducing Online Privacy Risks: Why Consumers Read (or don't read) Online Privacy Notices, Journal of Interactive Marketing, 18(3): 15–29.
Mitja, G., et al (eds.) (2014), The Italian Code of Criminal Procedure. Critical Essays and English Translation, CEDAM and Wolters Kluwer Italia.
Morsink, J. (2000), The Universal Declaration of Human Rights: Origins, Drafting and Intent, Pennsylvania Studies in Human Rights: Philadelphia: Univ. of Pennsylvania Press.
Nash, S. (2002), Balancing Convention Rights: P.G. and J.H. v United Kingdom in: The International Journal of Evidence & Proof, Vol 6, Issue 2, pp. 125 – 129.
Nissenbaum, H. (1997), Toward an Approach to Privacy in Public: Challenges of Information Technology, Ethics & Behavior, 7:3, 207-219.
Odinot, G. et al. (2017), Organised Cybercrime in the Netherlands: Empirical findings and implications for law enforcement, Dutch Ministry of Justice.

Copyright © Cyber-Trust Consortium. All rights reserved.

Papathanasiou, A. et al. (2014), Legal and Social Aspects of Cybercrime in Greece, E-Democracy, Security, Privacy and Trust in a Digital World (5th International Conference, E-Democracy 2013, Athens, Greece, 5-6 December 2013), Revised Selected Papers, Volume 441.
Popescul, D. and Georgescu, M. (2013), Internet of Things – Some ethical issues, researchgate.net
Quinn, P. (2016), D2.1 Report on the Data Protection, Privacy, Ethical and Criminal Law Framework Deliverable, FORENSOR project.
Reiman, J. (2004), Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posted by the Information Technology of the Future. In Privacies: Philosophical Evaluations, Stanford, Stanford University Press.
Roessler, B. (2006), New Ways of Thinking about Privacy. In Anne Philips Bonnie Honig & John Dryzek (eds.), Oxford Handbook of Political Theory. Oxford University Press. pp. 694-713.
Rosenberg, A. (2010), Virtual World Research Ethics and the Private/Public Distinction, International Journal of Internet Research Ethics, 3(1): 23–37.
Rubinstein, I.S. (2013), Big Data: The End of Privacy or a New Beginning? In International Data Privacy Law, Vol. 3, No. 2, pp.74-87.
Scanlon, T. (1975), Thomson on Privacy. Philosophy and Public Affairs 4.4: 315-322.
Smith, H.J., Dinev, T. and Xu (2011), H. Information Privacy Research: An Interdisciplinary Review, MIS Quarterly Vol.35 (4), pp. 989–1015.
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.
Solove, D. J. (2008), Understanding privacy. Cambridge, Mass: Harvard University Press.
Solove, D. J. (2011), Nothing to hide: The false tradeoff between privacy and security. New Haven [Conn.]: Yale University Press.
Tavani, T. H. (2009), Informational Privacy: Concepts, Theories, and Controversies in: The Handbook of information and Computer Ethics.
van Dijck, J. (2014), Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society 12(2): 197-208.
Volio, F (1981), Legal Personality, Privacy and the Family in Henkin (ed) The International Bill of Rights (Colombia University Press).
Wallace, K.A. (1999) Ethics and Information Technology 1: 21, Kluwer Academic Publishers.
Warren, S.D. & Brandeis, L.D. (1890), The Right to Privacy, Harvard Law Review, Vol. 4, No. 5, pp. 193-220.
Weber, A. M. (2003), The Council of Europe's Convention on Cybercrime, 18 Berkeley Tech. L.J. 425.
Westin, A. F. (1967), Privacy and freedom. New York: Atheneum.
Zouave, E. (2017), Law Enforcement Webcrawling: Lawfulness by Design and by Default, DANTE project, KU Leuven CiTiP.
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.

Case law

European Court of Human Rights

ECtHR, judgment of 6 September 1978, *Klass* and others v Federal Republic of Germany, appl.no. 1979-80.
ECtHR, judgment of 2 August 1984, Malone v. The United Kingdom, Judgment, appl.no. 8691/79.
ECtHR, judgment on Merits of 26 March 1987, Leander v Sweden, appl. no. 9248/81.
ECtHR, judgment of 12 July 1988, Schenk v. Switzerland, appl. no. 10862/84.
ECtHR, judgment on Merits of 24 April 1990, Huvig and Huvig-Sylvestre v France, appl. no. 11105/84.
ECtHR, judgment on merits of 24 February 1998, Botta v Italy, appl. no. 21439/9, Reports 1998-I.
ECtHR [GC], judgment of 16 February 2000, Amann v Switzerland, appl. no. 27798/95.
ECtHR [GC], judgment of 4 May 2000, Rotaru v Romania, appl. no 28341/95.
ECtHR, judgment of 28 January 2003, Peck v. United Kingdom, appl. no. 44647/98.
ECtHR [GC] judgment of 11 January 2006, Sørensen and Rasmussen v. Denmark, appl. nos. 52562/99 and 52620/99.
ECtHR, judgment of 26 October 2006, Khudobin v Russia, appl. no. 59696/00.

Copyright © Cyber-Trust Consortium. All rights reserved.

ECtHR [GC], judgment on Merits and Just Satisfaction of 2006, Jalloh v Germany, appl. no. 54810/00.
ECtHR [GC], Ramanauskas v Lithuania, judgment on Merits and just satisfaction of 5 February 2008, appl. no. 74420/01.
ECtHR, judgment of 4 December 2008, S. and Marper v. United Kingdom, appl. nos. 30562/04 and 30566/04.
ECtHR judgment of 8 January 2009, Schlumpf v. Switzerland, appl. no. 29002/06.
ECtHR, judgment on Merits and Just Satisfaction of 2009, Bykov v Russian Federation, appl. no. 4378/02.
ECtHR judgment of 15 January 2009, Reklos and Davourlis v. Greece, appl. no. 1234/05.
ECtHR judgment of 27 April 2010, Ciubotaru v. Moldova, appl. no. 27138/04.
ECtHR judgment of 27 April 2010, Vördur Olafsson v. Iceland, appl. no. 20161/06.
ECtHR [GC], judgment of 1 June 2010, Gäfgen v. Germany, appl. no. 22978/05.
ECtHR, judgement of 4 November 2010, Bannikova v. Russia, appl. no. 18757/06.
ECtHR, judgment of 8 August 2011, Heglas v. the Czech Republic, appl. no. 5935/02.
ECtHR, judgment on Merits and Just Satisfaction Case of 12 January 2016, Szabo and Vissy v Hungary, appl. no. 37138/14.
ECtHR, judgment of 19 June 2018, Centrum För Rättvisa v Sweden, appl. no. 35252/08.

Court of Justice of the European Union
CJEU, National Panasonic v Commission, Case 136/79 [1980] ECR 2033.
CJEU, Commission v Germany, Case C-62/90 [1992] ECR I-2575.
CJEU, Joined Cases C-92/09 and C- 93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, 9 November 2010.
CJEU, Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others, Judgment of the Court (Third Chamber), 7 November 2013, Case C-473/12.
CJEU, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Judgment of the Court (Grand Chamber), Joined Cases C-293/12 and C-594/12, 8 April 2014.
CJEU, Ryanair Ltd v PR Aviation BV, Judgment of the Court (Second Chamber), 15 January 2015, Case C-30/14.
CJEU, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, Judgment of the Court (Third Chamber) of 1 October 2015, Case C-230/14.
CJEU, Patrick Breyer v Bundesrepublik Deutschland, Judgment in Case C-582/14, Luxembourg, 19 October 2016.
CJEU, Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, Judgment of the Court (Grand Chamber) of 21 December 2016, Joined Cases C-203/15 and C-698/15.

UN Human Rights Committee
Coeriel et al. v. The Netherlands, Communication No. 453/1991, U.N. Doc. CCPR/C/52/D/453/1991 (1994).
Leo Hertzberg et al. v. Finland, Communication No. 61/1979, U.N. Doc. CCPR/C/OP/1 at 124 (1985).

Documents of International Organisations

United Nations
UN General Assembly, *Optional Protocol to the International Covenant on Civil and Political Rights*, 19 December 1966, United Nations, Treaty Series, vol. 999.

UN General Assembly, Report of the third Committee on the Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms, 8 December 2014, A/69/488/Add.2.

UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April 1988.

Copyright © Cyber-Trust Consortium. All rights reserved.

UN Human Rights Committee (HRC), *Concluding observations on the fourth periodic report of the United States of America*, 23 April 2014, CCPR/C/USA/CO/4.

UN Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Addendum, Communications to and from Governments*, 16 May 2011, A/HRC/17/27.

UN Human Rights Council, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development*, 29 June 2012, A/HRC/20/L.13.

UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,* 17 April 2013, A/HRC/23/40.

UN Human Rights Council, *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Right*s, OHCHR, U.N. Doc. A/HRC/27/37 (June 30, 2014).

Council of Europe

Council of Europe Committee of Ministers Recommendation No. R (87) 15 to the Member States on regulating the use of personal data in the police sector, 17 September 1987.

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

Council of Europe/European Court of Human Rights, Right to a fair trial. Article 6 of the Convention – Criminal law, 2014.

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

Council of Europe, Opinion on the Data protection implications of the processing of Passenger Name Records, T-PD (2016) 18 rev, 19 August 2016, Strasbourg.

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

Council of Europe, Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, home and correspondence, updated on 31 August 2018.

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

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

Other organisations

Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980.

a. Documents of European Institutions

Article 29 Data Protection Working Party

Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007, 01248/07/EN WP 136.

Copyright © Cyber-Trust Consortium. All rights reserved.

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, adopted on 2 April 2013, WP203.

Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, 844/14/EN WP 217.

Article 29 Data Protection Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, adopted on 16 September 2014, 14/EN WP 223.

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

Article 29 Data Protection Working Party, Working Document on surveillance of electronic communications for intelligence and national security purposes, adopted on 5 December 2014, 14/EN WP 228.

Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, adopted on 4 April 2017, 17/EN WP 248 rev.01.

Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted on 3 October 2017, 17/EN WP251rev.01.

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

Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (Directive 2016/680), adopted on 29 November 2017, 17/EN WP 258.

Article 29 Data Protection Working Party, Guidelines on Article 49 of Regulation 2016/679, adopted on 6 February 2018, 18/EN WP262.

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2018, 00264/10/EN WP 169.

Article 29 Data Protection Working Group, Guidelines on consent under Regulation 2016/679, Revised and Adopted on 10 April 2018, 17/EN WP259 rev.01

European Data Protection Board
European Data Protection Board (EDPB), Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018.

European Data Protection Board (EDPB), Statement on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, 28 May 2018.

European Data Protection Supervisor
European Data Protection Supervisor (EDPS), Guidelines on the Rights of Individuals with regard to the Processing of Personal Data, Brussels 2014.

European Data Protection Supervisor (EDPS), Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017.

Copyright © Cyber-Trust Consortium. All rights reserved.

European Data Protection Supervisor (EDPS), Jasmontaite, L. et al [Eds], Implementation of Data Protection by Design and by Default: Framing guiding principles into applicable rules, Vienna, 9 June 2017.

European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data, 11 October 2007.

European Commission

European Commission, Communication to the European Parliament and the Council on Promoting Data Protection By Privacy Enhancing Technologies (PETs), COM (2007) 228 Final, Brussels, 2 May 2007.

European Commission, Memo, Frequently Asked Questions: Data Retention, Brussels, 8 April 2014, available at: http://europa.eu/rapid/press-release_MEMO-14-269_en.htm [Accessed: 06.08.2018].

European Commission, DG Communications, Networks and Technology, EPrivacy directive, assessment of transposition, effectiveness and compatibility with the proposed data protection regulation, Digital Agenda for Europe, 2015.

European Commission, Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Brussels, 13.9.2017 COM (2017) 474 final.

European Commission, The Directive on security of network and information systems (NIS Directive), available at: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive [Accessed: 02.08.2018].

European Commission, Implementation of the NIS Directive in Italy, available at: https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-italy [Accessed: 01.08.2018].

European Commission, Implementation of the NIS Directive in The Netherlands, available at: https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-netherlands [Accessed: 28.08.2018].

European Commission, Transposition of the Directive (EU) 2016/680: State of play in the Member States, February 2018.

European Commission, Fact Sheet - Frequently Asked Questions: New EU rules to obtain electronic evidence, Brussels, 17 April 2018.

European Commission, Fact Sheet - July infringements package: key decisions, Brussels, 19 July 2018, available at: http://europa.eu/rapid/press-release_MEMO-18-4486_en.htm [Accessed: 27.08.2018].

Other institutions, bodies and agencies

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.

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.

Copyright © Cyber-Trust Consortium. All rights reserved.

European Union Agency for Fundamental Rights (FRA) and Council of Europe (CoE), Handbook on European Data Protection Law, 2018 edition.

European Union Agency for Fundamental Rights (FRA), Fundamental Rights Report 2017, Luxembourg 2017.

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), Privacy and Data Protection by Design - from policy to engineering, December 2014.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD).

European legislation

Council of Europe

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

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, *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.

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

European Union

Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, C/2018/0471, OJ L 26, 31.1.2018, p. 48–51.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995 P. 0031 – 0050.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, pp. 54–63.

Copyright © Cyber-Trust Consortium. All rights reserved.

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.

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.

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

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, *OJ L 194, 19.7.2016, p. 1–30.*

European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

Regulation (EU) 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, p. 9–12.

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

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p. 89–100.

Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 1–11.

Other sources

American Civil Liberties Union (2014), Privacy Rights in the Digital Age, A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights: A Draft Report and General Comment by the American Civil Liberties Union.

Association of Chief Police Officers, ACPO Good Practice Guide for Digital Evidence, March 2012.

ASU Alumni (2018), Why are human so obsessed with self-documenting?, asu.edu

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

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

Copyright © Cyber-Trust Consortium. All rights reserved.

Cameron, E. (2015), The Data Retention Saga: Dutch Court Declared National Data Retention Law Invalid, peacepalacelibrary.nl

Cobain, I., UK has six months to rewrite snooper's charter, high court rules, The Guardian, 27 April 2018.
Computer Incidence Response Center, TR-44 - Information security - laws and specific rulings in the Grand Duchy of Luxembourg, circl.lu

Crime Combating Department, Relevant Legislation, available at: http://www.police.gov.cy/police/police.nsf/All/D753CDF2D439A9EAC225829C003B75D4?OpenDocument [Accessed: 06.08.2018].

Cybersecurity and NIS Directive: the Italian implementing Decree, 29 June 2018, blblex.it

David, D., Bills designed to implement the General Data Protection Regulation in Luxembourg, 5 September 2017, castegnaro.lu

Davidson, A., Increasing trust in criminal evidence with blockchains, 2 November 2017, gov.uk

Electronic Frontier Foundation and Article 19 (2014), Necessary and proportionate: International Principles on the Application of Human Rights Law to Communications Surveillance, Background and Supporting International Legal Analysis, available at: http://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf [Accessed 20.07.2018].

EU Network of independent experts on fundamental rights, Commentary on the European Charter of the Fundamental Rights of the European Union, June 2006.

Executive Office of the President of the United States, “Big Data: Seizing Opportunities, Preserving Values”, May 2014.

Fair Trials International, Third Party Intervention in the ECtHR, Application No. 30460/13, March 2014.

Gkotsopoulou, O. (2015), How big is your privacy in a big data world?, unpublished manuscript, Europa Universität Viadrina.

Filippone, R. Blockchain and individuals’ control over personal data in European data protection law, Tilburg University, August 2017.

Graceful, H., UK Cyber Crime Law, 15 June 2016, gracefulsecurity.com

Hill, K. (2014), Facebook Added ‘Research’ To User Agreement 4 Months After Emotion Manipulation Study, Forbes.com.

Information Commissioner´s Office (ICO), Guide to law enforcement provisions, 7 December 2017, pdpjournals.com

Information Commissioner´s Officer (ICO), What is personal data, ico.org.uk.

Kalis, P., NIS Directive – update for the Netherlands, Leiden Law Blog, 31 January 2018.

Macnish, K. Surveillance Ethics, Internet Encyclopaedia of Philosophy, iep.utm.edu

Maldoff, G., Top 10 operational impacts of the GDPR: Part 8 – Pseudonymization, 12 February 2016, iapp.org

Copyright © Cyber-Trust Consortium. All rights reserved.

Maldoff, G., How GDPR changes the rules for research, 19 April 2016, iapp.org

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

Privacy International, Victory! UK Surveillance Tribunal Finds GCHQ-NSA Intelligence Sharing Unlawful, (available at: https://www.privacyinternational.org/?q=node/485 [accessed July 24, 2018]).

Rands, K., How blockchain is disrupting the legal industry, Global Legal Blockchain Consortium, 9 June 2018

Rezai, A., Beware of the Spiders: Web Crawling and Screen Scraping – the Legal Position, 6 February 2017, parissmith.co.uk

The Crown Prosecution Service, Computer Misuse Act 1990 - Legal Guidance: Cyber / online crime, cps.gov.uk

UK Government services, Data Protection Bill: implementing the European Union Law Enforcement Directive No: HO0295, gov.uk.

UK Home Office, Dept for Digital, Culture, Media and Sports, Data Protection Bill Factsheet – Law enforcement processing (Clauses 29–81), gov.uk

Copyright © Cyber-Trust Consortium. All rights reserved.