CANVAS – Constructing an Alliance for Value-driven Cybersecurity

White Paper 2

Cybersecurity and Law

Lina Jasmontaite, *Vrije Universiteit Brussel**
Gloria González Fuster, *Vrije Universiteit Brussel**
Serge Gutwirth, *Vrije Universiteit Brussel**

Florent Wenger, *Université de Lausanne*
David-O. Jaquet-Chiffelle, *Université de Lausanne*
Eva Schlehahn, *Unabhängiges Landeszentrum für Datenschutz Schleswig - Holstein*

This report consolidates the findings of Work Package 2 of the CANVAS Support and Coordination Action; * Work Package Leader

The CANVAS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540.

This work was supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1. The opinions expressed and arguments employed therein do not necessarily reflect the official views of the Swiss Government.

Content

Executive Summary

This White Paper explores the legal dimensions of the European Union (EU)'s value-driven cybersecurity by investigating the notions of 'value-driven' and 'cybersecurity' from the perspective of EU law. It starts with a general overview of legal issues in current value-driven cybersecurity debates (Chapter 2), showing how values embedded within the framework of EU governing treaties have evolved during the integration process, and the important role they play in the cybersecurity regulation at EU level.

Chapter 3 of the White Paper is devoted to the main critical challenges in this area: 1) the varied and sometimes unclear uses of the term 'cybersecurity', 2) the roles of stakeholders and the cooperation between them, and the 3) securitization of EU values and interests through cybersecurity rules.

Chapter 4 points out and describes specific controversies concerning cybersecurity regulation in the EU. Ten disputed issues are given particular attention: 1) the functioning of human rights as drivers for EU regulation, 2) the regulation of risks to society through individual risk identification and proactive action, 3) the attribution of roles to different stakeholders, 4) how individuals are being awarded with more rights, 5) controllership of data, 6) copyright protection, 7) regulation of online content, 8) the use of encryption, 9) permissibility of massive and generalised surveillance of individuals and 10) counterterrorism measures.

Chapter 5 summarises the main findings of the literature review. The White Paper recognises that legislative and policy measures within the cybersecurity domain challenge EU fundamental rights and principles, stemming from EU values. The White Paper concludes that with the constantly growing number of EU measures governing the cybersecurity domain, the embedment of EU values enshrined in the EU Charter within these measures take place both on an *ex ante* and an *ex post* basis.

This White Paper is based on the input provided by CANVAS project partners that is included in Annexes as follows:

- Annex I includes a review of EU soft-law measures addressing and surrounding cybersecurity issues.
- Annex II lists EU legislative measures on cybersecurity issues.
- Annex III discusses cybersecurity and criminal justice affairs.
- Annex IV is devoted to the discussion of cybersecurity, privacy and data protection matters.
- Annex V provides an overview of cybersecurity definitions developed in national cybersecurity strategies of 18 EU Member States.
- Annex VI provides a brief description of EU values listed in the EU governing treaties.

CANVAS White Papers – Overview

In order to summarize the existing literature on the topics and issues that are relevant for the CANVAS project, the CANVAS consortium has created four White Papers as follows:

- White Paper 1 – Cybersecurity and Ethics: This White Paper outlines how the ethical discourse on cybersecurity has developed in the scientific literature, which ethical issues gained interest, which value conflicts are discussed, and where the "blind spots" in the current ethical discourse on cybersecurity are located. The White Paper is based on an extensive literature with a focus on three reference domains with unique types of value conflicts: health, business/finance and national security. For each domain, a systematic literature search has been performed and the identified papers have been analysed using qualitative and quantitative methods. An important observation is that the ethics of cybersecurity not an established subject. In all domains, cybersecurity is recognized as being an instrumental value, not an end in itself, which opens up the possibility of trade-offs with different values in different spheres. The most prominent common theme is the existence of trade-offs and even conflicts between reasonable goals, for example between usability and security, accessibility and security, privacy and convenience. Other prominent common themes are the importance of cybersecurity to sustain trust (in institutions), and the harmful effect of any loss of control over data.
- White Paper 2 – Cybersecurity and Law: This White Paper explores the legal dimensions of the European Union (EU)'s value-driven cybersecurity. It identifies main critical challenges in this area and discusses specific controversies concerning cybersecurity regulation. The White Paper recognises that legislative and policy measures within the cybersecurity domain challenge EU fundamental rights and principles, stemming from EU values. Annexes provide a review on EU soft-law measures, EU legislative measures, cybersecurity and criminal justice affairs, the relation of cybersecurity to privacy and data protection, cybersecurity definitions in national cybersecurity strategies, and brief descriptions of EU values.
- White Paper 3 – Attitudes and Opinions regarding Cybersecurity: This White Paper summarises currently available empirical data about attitudes and opinions of citizens and state actors regarding cybersecurity. The data emerges from reports of EU projects, Eurobarometer surveys, policy documents of state actors and additional scientific papers. It describes what these stakeholders generally think, what they feel, and what they do about cyber threats and security (counter)measures. For citizens' perspectives, three social spheres of particular interest are examined: 1) health, 2) business, 3) police and national security.
- White Paper 4 – Technological Challenges in Cybersecurity: This White Paper summarizes the current state of discussion regarding the main technological challenges in cybersecurity and impact of those, including ways and approaches to addressing them, on key fundamental values. It provides an overview on current cybersecurity threads and countermeasures and focuses on ethical dilemmas that emerge when counteracting those threads. It also points to the fact that the cybersecurity community relies much more on interpersonal relations when sharing intelligence and data than in explicit national or supranational regulations. Furthermore, the White Paper presents advanced cryptographic techniques and data anonymization techniques that may help to solve or minimize some of the ethical dilemmas.

All White Papers and additional material are available at the Website of the CANVAS project: ww.canvas-project.eu

1. Introduction

The aim this White Paper is **to summarize** the current state of **discussions** on **value-driven cybersecurity and EU law**, granting special attention to issues of criminal justice and the protection of individuals' rights to privacy and personal data. It outlines main challenges, positions and identifies legal mechanisms for incorporating EU fundamental rights into regulatory measures and policies.

In preparation for the main part of the White Paper, which summarises findings of the literature research, six annexes were developed. Annex I includes a review of EU soft-law measures addressing and surrounding cybersecurity issues. Annex II lists the existing EU legislative measures concerning cybersecurity. Annex III discusses cybersecurity and criminal justice affairs; and Annex IV is devoted to the discussion of cybersecurity, privacy and data protection matters. Annex V outlines cybersecurity definitions developed in national cybersecurity strategies of 18 EU Member States. Annex VI provides a brief description of EU values listed in the EU governing treaties.

The White Paper at hand has been prepared in the context of Work Package 2 (WP2) of the CANVAS project. It aims at providing input for the CANVAS workshops, to be organised within the scope of Work Package 5 (WP5) and dissemination activities foreseen in Work Packages 6, 7 and 8 (WP6, WP7 and WP8). It will also be made publicly available and accessible for interested stakeholders on the CANVAS website.

1.1 Methodology

The **literature research** presented in the main part of White Paper as well as Annexes III and IV entailed analysis of key EU legal and policy documents, working papers, guidelines issued by relevant authorities, academic literature and jurisprudence in the specific area at stake.

The White Paper also specifies ten common controversies in the domain of cybersecurity and law (see Chapter 4), with a specific focus on a) criminal justice and b) privacy and personal data protection – the two areas that stand out as a key challenge for EU value-driven cybersecurity. In order to identify the main controversies out of numerous controversies that emerged during the literature review, **five semi-structured interviews** with representatives of different stakeholder groups were conducted during the period of June 7- 14 June, 2017. A list of questions on fairly specific topics was developed with an aim to **complement literature research**.[1] The questions were formulated in such a way they could help answering research questions (e.g., What controversies could be identified in the domain of cybersecurity?). The list of questions served as an interview guide; questions followed a reasonable order that allowed interviewers 'to glean the ways in which research participants view their social world', which in this particular case has been shaped by their expertise and experience in the domain of cybersecurity.[2] The selected form of interviews allowed for **a flexible process** during which the interviewer could pick up on things that were said by interviewees.[3] This particular way of carrying out interviews allowed understanding interviewees in a better way as they would be given an opportunity not only to position themselves within the field of cybersecurity or a particular issue but also to explain rationale behind their positions.

The selected interviewees can be considered to represent different groups of major stakeholders in the domain of cybersecurity in the EU, namely policy makers and regulators, technology developers, IT experts, academia, and business. Interviews with representatives of different stakeholder groups proved

[1] Bryman, A., *Social Research Methods*, Oxford University Press, 2008, 438.
[2] Ibid., 442.
[3] Ibid., 442.

to be valuable as they facilitated the creation of a list that entails major controversies of cybersecurity laws in the EU.

The White Paper starts with a general **overview of legal issues** in current **value-driven cybersecurity discussions** (Chapter 2). The following Chapter 3 of the paper is devoted to **challenges related to regulation of cybersecurity**. Particular attention is granted in this chapter to criminal justice and protection of privacy and personal data protection law. Then, Chapter 4 points out **controversies concerning cybersecurity regulation in the EU**. While doing so, the fourth chapter outlines positions and arguments currently at stake, and identifies existing and up-coming legal mechanisms for incorporating EU fundamental rights into innovation and policies.

2. Delimiting Cybersecurity in the EU

There have been numerous attempts to define cybersecurity from a scientific, technical, political or legal point of view.[4] Many definitions focusing on different dimensions of cybersecurity (e.g., political, military, economic, technical, legal and citizens') have been proposed by different actors, yet there is no single definition which fully captures the complexity of the matter at stake. As explained by the European Union Agency for Network and Information Security (ENISA) in its 2015 report *Definition of Cybersecurity: Gaps and overlaps in standardization*, cybersecurity is a broad and evolving term and therefore, the use of '***a contextual definition***' of its meaning should always be privileged.[5] The ENISA report noted that while opting for a specific definition can allow maintaining clarity, stakeholders and policy makers should select definitions that fit their particular needs.[6] In practice, this means that ENISA does not propose any definition of 'cybersecurity' that could be shared by various stakeholders and policy makers, including EU institutions. Rather, it recommends adopting interpretations developed by standardisation organisations, such as the European Committee for Electrotechnical Standardization (CENELEC) and the International Organization for Standardization (ISO), or international organisations, such as the International Telecommunication Union (ITU).

According to ITU, cybersecurity means '*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets*'.[7] Although this definition may appear extremely broad, and despite the fact that definitions related to technical requirements may serve better during a negotiation phase, it is important to consider that definitions developed by standardisation organisations target the micro-management level. Therefore, they may carry a risk of conceptualising 'cybersecurity' in an unduly limited way. For example, cybersecurity may be seen only as a concern of risk that may arise online, it may be understood as a protection of only virtual assets, or it may only target malicious activities.

Definitions adopted by different organisations typically represent different points of view, and can potentially be at odds with each other. For example, some frame cybersecurity as a mere technical issue, whereas Member States in their national security strategies may regard cybersecurity as an issue of national security.[8] The latter view may hamper the development of regulatory measures governing this particular area by the EU. Pressed by this concern, the EU legislator favours understandings in line with its objectives and competences, as outlined in Articles 4 and 5 of the Treaty on European Union (TEU).[9] It has chosen to employ a definition according to which '*[c]ybersecurity commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields,*

[4] For example, EU Member States tend to adopt their own definitions of cybersecurity; an overview of these definitions is provided in Annex V; an overview of technical definitions for the term 'cybersecurity' is provided in ENISA, Definition of Cybersecurity: Gaps and overlaps in standardization, December 2015, see further: Craigen, D., Diakun-Thibault, N., Purse, R., 'Defining Cybersecurity', Technology Innovation Management Review 2014, 4(10), 13-21; Adams, S., Brokx, M., Dalla Corte, L., Galic, M., Kala, K., Koops, B. J., Skorvánek, I. (2015). The governance of cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK. Tilburg University.

[5] ENISA, Definition of Cybersecurity: Gaps and overlaps in standardization, December 2015, 7.

[6] Ibid., 28.

[7] ITU, Recommendation, ITU-T X.1205, p. 2, ENISA, Definition of Cybersecurity: Gaps and overlaps in standardization, December 2015, 16-17.

[8] For example, according to Ireland's National Cyber Security Strategy 2015-2017 'The Government's Cyber Security Strategy sets out how Ireland will protect and improve the cybersecurity of Critical National Infrastructure in the context of national emergency planning'.

[9] According to Article 4.2 of the TEU, the EU recognises that issues related to 'national security remains the sole responsibility of each Member State'.

from those threats that are associated with or that may harm its interdependent networks and information infrastructure'.[10] In this context, cybersecurity's primary objective is described 'to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein'.[11] In the following section the EU approach to cybersecurity regulation is presented in greater detail.

2.1 The EU and Cybersecurity

In 2013, the European Commission and the High Representative of the EU for Foreign Affairs and Security Policy published a joint communication presenting a Cybersecurity Strategy for the EU (EU Cybersecurity Strategy or 2013 Strategy), aiming '*to make the EU's online environment the safest in the world*'.[12] The 2013 Strategy identified five strategic priorities, namely:[13]

- Achieving cyber resilience by establishing minimum requirements for the functioning, cooperation and coordination of national competent authorities for network information systems.
- Drastically reducing cybercrime by 1) ensuring swift transposition of the cybercrime related Directives, 2) encouraging ratification of the Budapest Convention on Cybercrime, and 3) developing funding programs for the deployment of operational tools.
- Developing a cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP) by 1) assessing operation EU cyberdefence requirements, 2) developing the EU cyberdefence policy framework, 3) promoting dialogue and coordination between civilian and military actors in the EU, and 4) facilitating a dialogue with international partners.
- Developing the industrial and technological resources for cybersecurity by 1) establishing a public-private platform on NIS (Network and Information Security) solutions, 2) providing technical guidelines and recommendations for the adoption of NIS standards and good practices, and 3) encouraging the development of security standards for technology 'with stronger, embedded and user-friendly security features'.
- Establishing a coherent international cyberspace policy for the EU and promoting core EU values by mainstreaming cyberspace issues into EU external relations and Common Foreign and Security Policy (CFSP), and by supporting capacity building on cybersecurity and resilient information infrastructures in third countries. More specifically, the EU should ensure that its consultations with international partners on cyber issues are designed to complement the existing bilateral dialogues between the Member States and third countries. These consultations shall be driven by the EU core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights. Following the objectives of this priority, the EU aims at attaining a high level of data protection, including protection of personal data transfers to third countries.

The 2013 Strategy built on previous initiatives and sectorial frameworks, such as the legal frameworks for telecommunications, electronic commerce and electronic signatures, policy and regulatory measures, which have traditionally delineated the fragmented landscape of EU's approach to cybersecurity. The section below provides an overview of major policy documents that allowed advancing discussions on cybersecurity in the EU. Major legislative measures are listed in Annex II of this document.

In autumn 2017, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy published a Joint Communication to the European Parliament and the Council of the European Union titled '*Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*'.

[10] European Commission and High Representative of the EU for Foreign Affairs and Security Policy (2013), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final, 3.
[11] Idem.
[12] Idem.
[13] Ibid., 4-16.

This Joint Communication reaffirms policy objectives set in the EU Cybersecurity Strategy and it puts forward a set of step-by-step actions and measures that would allow 1) building greater EU resilience to cyber-attacks, 2) facilitating **detection of cyber-attacks**, and 3) strengthening **international cooperation on cybersecurity**. In particular, the Joint Communication 'calls for more robust and effective structures to promote cybersecurity and to respond to cyber-attacks in the Member States but also in the EU's own institutions, agencies and bodies. It also requires **a more comprehensive**, **cross-policy approach** to building **cyber-resilience** and strategic autonomy, with a strong Single Market, major advances in the EU's technological capability, and far greater numbers of skilled experts'. [14]

2.2 Soft-law Paved the Way for Hard-law Addressing Cybersecurity

As noted by Van der Meulen et al. 2015, in the last two decades the **EU** has not only been asserting itself as **a prominent security actor**, but it has also produced a significant amount of **new regulation**, initiatives and sectorial frameworks tackling issues arising from active use of information systems and networks.[15] Studying legislative measures without taking into account **the wider context** in which they were developed provides little insight into the debates underpinning their adoption, and it is therefore useful to also analyse **EU soft-law measures** (e.g., communications and strategies) that addressed issues related to cybersecurity.[16] Therefore, in order to better understand how the EU regulatory approach towards cybersecurity has evolved over the years, it is important to reflect on EU soft-law.

The review of EU soft-law measures, in particular policy documents, related to information systems and networks security allows establishing six observations. **The review is included in Annex I** of this White Paper and it presents EU policy documents, such as communications, Council resolutions and implementation reports that address issues of information systems and networks security. The reviewed documents cover the period of 2000-2016. The selected documents are presented in chronological order as this particular structure of the review allows tracking down the development of EU cybersecurity policy, including the emergence of the term 'cybersecurity'. In order to find the first documents addressing issues related to cybersecurity, the authors relied on references included in policy documents to earlier documents, which are followed up, related or addressed similar issues. All of the reviewed documents are available in EU bibliographical databases and can be accessed on the Internet.

1. First, the EU has **not yet** developed **a holistic approach of cybersecurity protection**, despite early calls for a comprehensive action.[17] Relevant policy documents as well as legislative measures are found within frameworks addressing 1) **network and information security** measures (targeting operators of essential services, and providers of critical and digital infrastructures), 2) **electronic communications** (which includes privacy and data protection issues), and 3) **cybercrime**. The **blurring boundaries** between the three policy areas are raising questions with regard to the EU approach to cybersecurity regulation. A hypothetical example of blurring boundaries could include a situation, where an abuse of network and information security measures on a critical infrastructure results in a cybercrime, which in turn triggers the involvement of law enforcement authorities. Whilst consulting legislative acts in the three policy areas may be feasible, information sharing of different authorities involved in this case may be a formidable task. Therefore, establishing clear rules for evidence collection and sharing among competent authorities as well as for law

[14] European Commission and High Representative of the EU for Foreign Affairs and Security Policy (2013), Joint Communication to the European Parliament, the Council, 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', JOIN(2017) 450 final, 2017, 3.

[15] Van der Meulen Nicole, Eun A. Jo and Stefan Soesanto (RAND Europe), Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses (2015), available at: http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)536470.

[16] The detailed analysis of these documents is included in Annex I.

[17] European Commission, Communication 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime', COM(2000) 890.

enforcement cooperation with the private sector are crucial.[18] Additionally, the development of 'best-practice systematic approaches to software and hardware design and development' for all IT systems, as suggested by High Level Group of Scientific advisors, may help to overcome the fragmented regulatory approach.[19]

2. Second, the area of cybersecurity emerged gradually as a result of the **EU responsive regulation approach**.[20] Similarly to other policy areas subjected to the responsive regulation approach, EU policy documents on cybersecurity firstly identified **undesirable situations** (e.g., lack of infrastructure, digital skills or trust in online service providers). Then, in response to these undesirable situations or conditions various measures were proposed. Often these measures were framed as strategies (e.g., Cybersecurity Strategy of the European Union or Digital Single Market Strategy) or agendas (e.g., The Digital Agenda for Europe) with priority lists and specific action plans; the implementation of these action plans is evaluated after a certain period of time. Then, if necessary, the measures addressing the undesirable situations or conditions are revised and modified.

3. Third, **issues concerning cybersecurity**, such as protection of information systems and energy supply, were first **brought in by the EU Member States** within the scope of **debates on security** at **the Council of EU**. Building on this observation, it can be suggested that cybersecurity regulation in the EU has **advanced** mainly due to the **political pressure** from Member States. Explicit references to 'cybersecurity' can be found only in EU soft-law documents. The Digital Agenda for Europe Scoreboard 2012 and the Special Eurobarometer study, 'Cyber security', were among the first documents that introduced the term 'cybersecurity' in order to address various issues related to the digital environment.[21] The term 'cybersecurity' in its more comprehensive sense to the EU discussions (i.e., going beyond cybercrime) was brought in after the adoption of EU Cybersecurity Strategy in 2013. In measures that are directly addressed to the Member States, the EU is reluctant to use this term, preferring the term 'security of information systems and networks'. This **careful choice of wording** may suggest that there is a 'competence problem', which is pivotal to the relationship between the EU and its Member States.[22] But it would be more accurate to suggest that the EU competence in the field of cybersecurity is still taking shape. As per Craig, **EU competence** represents **a synergetic interaction** of: EU competence that has been conferred to it by the Member States; Member States and the European Parliament acceptance of legislation that has given substance to the Treaty articles; EU jurisprudence; and the interpretation of EU competence by the institutions.[23]

4. Fourth, from the inception of debates about cybersecurity protection, the importance of **incorporating fundamental rights of individuals** in EU policy and regulatory measures has been **emphasised.** For example, the Stockholm Program, a follow up of the European Security Strategy developed in 2003, while claiming that '*law enforcement measures and measures to safeguard individual rights, the rule of law, international protection rules [should] go hand in hand in the same direction*', emphasised that the **EU carries a duty** to '*respond to the challenge posed by the increasing exchange of personal data and the need to ensure the protection of privacy*'.[24] This claim surfaces in several other policy documents, even it has received little attention in the literature.

5. Fifth, the **objectives** of relevant **EU policies** have remained **practically invariable** for almost two

[18] European Commission, Communication 'The European Agenda on Security', COM(2015) 185 final, 19-20.
[19] High Level Group of Scientific Advisors, Cybersecurity in the European Digital Single Market. SAM, Scientific Opinion No. 2/2017 March 2017.
[20] For more about responsive regulation see: Baldwin R., Black J., 'Really Responsive Regulation', 2008, Modern Law Review 71, 59-74.
[21] European Commission, Communication 'The Digital Agenda for Europe - Driving European growth digitally', COM(2012) 784 final and Special Eurobarometer 390, Cyber security, Wave EB77.2 – TNS Opinion & Social, 2012.
[22] Craig, P., *The Lisbon Treaty: law, politics, and Treaty reform*, Oxford University Press, 2013, 156.
[23] Ibid.
[24] Council of the EU, The Stockholm Program: An open and secure Europe serving the citizen, 17024/09 (2009), 3.

decades. For example, the EC Communication 'eEurope 2002: Impact and Priorities', which was an integral part of the Lisbon Strategy, stressed the need to enhance user confidence in the field of electronic commerce by 1) providing **support to industry-led security certifications** through co-ordination of efforts and mutual recognition; 2) promoting **privacy-enhancing technologies**, including proper codes and the consolidation of practice; and 3) stimulate **public/private cooperation** on dependability of information infrastructures. These themes are also addressed among the strategic priorities and actions of the EU Cybersecurity Strategy. They are also echoed in the 2016 Communication 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry'.

6. Lastly, there was also **a shift in security thinking** in relation to **cybersecurity**. In this sense, early documents concerning cybersecurity used a generic understanding of threats and encouraged their exploration and identification,[25] whereas the **current legal and policy documents** tend to frame debates in terms of **risks**.[26]

2.3 EU Values

The political motivation for establishing the European Economic Community (now the EU) was driven by the need **to ensure security** (i.e., peace) of European nations after the Second World War. It was deemed that security could be achieved by creating an economic interdependency. In 1950 the Schuman declaration laid down a proposal to establish an oversight mechanism for a Franco-German production of coal and steel, the main materials that were used in the military sector.[27] The participation in this mechanism would be open to other countries. Following up on the objectives laid down in the Schuman declaration, three treaties have been developed, namely: the Treaty establishing the European Coal and Steel Community; the Treaty establishing the European Economic Community (EEC); and the Treaty establishing the European Atomic Energy (Euratom). All of the initial treaties referred to **economic objectives**, such as economic expansion, the development of employment and raising the standard of living instead of referring to particular values.[28] It can be suggested that the notion of EU values has morphed out in the debates about **EU objectives**, which are listed in Article 3 of TEU, during the successive treaty revision processes.[29] This list **no longer** focuses **exclusively** on **economic** objectives. According to the current governing treaties, the core EU objectives include the promotion of peace, EU values and the **well-being of its people**.[30]

Since the entry into force of the **Lisbon Treaty**, a detailed list of EU values can be found in **Article 2 of the TEU**. According to this article, '*[t]he Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities*'.[31] The following sentence of same article, explains that '*[t]hese values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail*'.[32] In other words, this means that the EU values

[25] For example, as a result of European Commission, Communication 'eEurope Benchmarking Report - eEurope 2002', COM/2002/0062 final, a cyber security task force was established.
[26] For example, the NIS Directive and the GDPR require to take into account risks associated with the processing of data when deciding upon appropriate technical and organization measures.
[27] The Schuman Declaration, 9 May 1950, available at: https://europa.eu/european-union/about-eu/symbols/europe-day/schuman-declaration_en.
[28] Treaty Constituting the European Coal and Steel Community, available at: http://www.consilium.europa.eu/uedocs/cmsUpload/Treaty%20constituting%20the%20European%20Coal%20and%20Steel%20Community.pdf.
[29] Steiner, J., Woods, L. *EU Law*, Oxford University Press, 2012, 51.
[30] Consolidated Version of the Treaty on European Union and the Treaty on the Functioning of the European Union (2010/C 83/01); The Treaty on European Union (TEU), Article 3 (1).
[31] Ibid., Article 2.
[32] Idem.

are determined by the principles of pluralism, non-discrimination, tolerance, justice and equal treatment of men and women.

The same message is echoed in the **EU Charter**, which as of the entry into force of the Lisbon Treaty has become **legally binding**. The Preamble of EU Charter claims that the EU is founded on common and '***universal values*** *of human dignity, freedom, equality and solidarity'.* Furthermore, *'[t]he Union contributes to the preservation and to the development of these common values while respecting the diversity of the cultures and traditions of the peoples of Europe as well as the national identities of the Member States and the organisation of their public authorities at national, regional and local levels; it seeks to promote balanced and sustainable development and ensures free movement of persons, services, goods and capital, and the freedom of establishment*.'[33] The EU Charter observes that in order to attain these objectives '*it is necessary to strengthen the protection of fundamental rights in the light of changes in society, social progress and scientific and technological developments by making those rights more visible in a Charter*.'[34]

Treaty of the EU, Article 2	Charter of Fundamental Rights of the EU, Preamble	EU values
Human dignity	Human dignity	Human dignity
Freedom	Freedom	Freedom
Democracy	Democracy	Democracy
Equality (including equality between women and men)	Equality	Equality
Non-discrimination	The rule of law	Non-discrimination
The rule of law	Solidarity	The rule of law
Respect for human rights (including the rights of persons belonging to minorities)	Protection of individuals by establishing the citizenship of the Union and by creating an area of freedom, security and justice	Respect for human rights
Pluralism		Pluralism
Tolerance		Tolerance
Justice		Justice
Solidarity		Solidarity
		Protection of EU citizens

Table 1: *Overview of values that are emphasized in the EU context. A brief description of each notion is provided in Annex VI of this White Paper.*

2.4 EU Values in External Action

For a better understanding of **EU values** as established by EU treaties, Article 2 of the TEU should be connected with the provisions governing the EU external relations, namely Article 3(5) and Article 21 of the TEU.

According to Article 3(5) of the TEU, '*[i]n its relations with the wider world, the Union shall uphold and promote its values and interests and contribute to the protection of its citizens. It shall contribute to peace, security, the sustainable development of the Earth, solidarity and mutual respect among peoples,*

[33] Consolidated Version of the Treaty on European Union and the Treaty on the Functioning of the European Union (2010/C 83/01); The EU Charter, Preamble, § 2 and 3.
[34] Ibid., § 4.

free and fair trade, eradication of poverty and the protection of human rights, in particular the rights of the child, as well as to the strict observance and the development of international law, including respect for the principles of the United Nations Charter.' [35]

According to Article 21 of the TEU, '*1. **The Union' s action on the international** scene shall be guided by the **principles** which have inspired **its own creation, development and enlargement**, and which it seeks to advance in the wider world: democracy, the rule of law, the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity, the principles of equality and solidarity, and respect for the principles of the United Nations Charter and international law. […]*

2. The Union shall define and pursue common policies and actions, and shall work for a high degree of cooperation in all fields of international relations, in order to:

(a) safeguard its values, fundamental interests, security, independence and integrity;

(b) consolidate and support democracy, the rule of law, human rights and the principles of international law;

(c) preserve peace, prevent conflicts and strengthen international security, in accordance with the purposes and principles of the United Nations Charter, with the principles of the Helsinki Final Act and with the aims of the Charter of Paris, including those relating to external borders […].'[36]

2.5 EU Values in Cybersecurity

According to the 2013 EU Cyber Security Strategy, '***the same norms, principles and values that the EU upholds offline, should also apply online***'.[37] In other words, the protection of fundamental rights, democracy and the rule of law are the key priorities in cyberspace, similarly to the offline world. When addressing the issues related to the protection of fundamental rights, the EU Cyber Security Strategy emphasizes that '*cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values*'.[38] The EU Cyber Security Strategy notes that safe networks and information systems can contribute to the protection of individuals' rights. In particular, information-processing operations for the purposes of cyber security should not undermine the rights to the freedom of expression, personal data and privacy. The Strategy recognizes that cybersecurity is a shared responsibility and therefore democratic and efficient multi-stakeholder governance, in which public and private parties are represented, should be ensured.

EU values shall guide EU institutions and Member States when representing EU interests in the international context, for example, at meetings with representatives of third countries or at international organisations, such as the Council of Europe (CoE), the Organisation for Economic Co-operation and Development (OECD), the Organization for Security and Co-operation in Europe (OSCE), the North Atlantic Treaty Organization (NATO) or the United Nations (UN).[39] Brazil, China, India, Japan, the Republic of Korea and the United States are considered to be EU strategic partners for cooperation on cyber policy and security of information and communication technologies.[40]

[35] TEU, Article 3(5).
[36] Ibid., Article 21.
[37] European Commission and High Representative of the EU for Foreign Affairs and Security Policy (2013), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final, 1.
[38] Ibid., 4.
[39] European Commission, Commission Staff Working document 'Comprehensive Assessment of EU Security Policy accompanying the document Communication to the European Parliament, the European Council and the Council: Ninth progress report towards an effective and genuine Security Union' (Part 1), Brussels, 26.7.2017 SWD(2017) 278 final, 78.
[40] Idem.

2.6 Why do Values Matter?

Values and governing principles may motivate decisions at various levels, and decisions related to policy, and legislation are no exception. Indeed, decisions are not value neutral and exemplify value driven choices, the influence of which can be analysed. Legal values are notably expressed in fundamental rights and principles. These values shape the legislator and the judiciary's functioning, and may also affect they way specific legal, societal and ethical issues are conceptualized and perceived. In the EU, these values, embodied by fundamental rights and principles, are found in the European Convention of Human Rights, the EU Charter of Fundamental Rights, and the EU Treaties.

The commitment to protect human rights is included in EU Treaties next to the objective to promote scientific and technological advance.[41] This commitment was further strengthened by awarding the EU Charter of Fundamental Rights with a legally binding status in Article 6 (1) of the TEU. The third paragraph of that article also recognizes '*fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights [ECHR] and Fundamental Freedoms […] shall constitute general principles of the Union' s law*' and foresees the accession to the ECHR in Article 6 (2) of the TEU. Consequently, the EU, in addition to a duty to give reasons for its legislative measures, as foreseen in Article 296 of the TFEU, is obliged to make sure that any legal act (e.g., regulations, directives, recommendations, decisions or opinions) it develops is in compliance with the set of rights enshrined in the EU Charter of Fundamental Rights, taking also into account the ECHR and constitutional traditions of the Member States.

Nevertheless, value-driven EU cybersecurity regulation is not always a reality. For example, Kuner points out that some principles embedded in the EU legislative acts pursuing its values, such as a system of representatives foreseen in Data Protection Directive (Directive 95/46/EC) for data controllers established outside the EU, have been not implemented in practice.[42] Kuner also argues that while EU proclaims its values as '*universal, global standards for the Internet*' without considering values of other countries or regions, only a large-scale empirical study could help to determine what EU values are actually reflected in practice.[43]

[41] TEU, Article 3.
[42] Kuner, C., 'The Internet and the Global Reach of EU Law' (February 1, 2017). Forthcoming, Collected Courses of the Academy of European Law (Oxford University Press); LSE Legal Studies Working Paper No. 4/2017; University of Cambridge Faculty of Law Research Paper No. 24/2017. Available at: http://dx.doi.org/10.2139/ssrn.2890930, 31.
[43] Ibid., 29-31.

3. Challenges of Cybersecurity Regulation

Technology, including ICT, continuously evolves and so do the opportunities and challenges it creates. Much has been written about the opportunities that technologies create in terms of economic growth, employment and inclusiveness.[44] This section outlines the **three main challenges that cybersecurity regulation faces in the EU**. With the revision of the first EU Cybersecurity Strategy scheduled for September 2017[45] and ongoing discussions about the mandate of ENISA, [46] the future of cybersecurity regulations appears to be at a crossroad – perceived cyber threats may shape political choices and lead to deeper integration or the creation of a Security and Defence Union.[47]

3.1 Ambiguous Use of the 'Cybersecurity' Concept

As described earlier, although numerous policies and regulatory measures have been adopted in order to advance the security of citizens, businesses and public administrations in the digital environment, there is **no single definition of the term 'cybersecurity' at EU level**. In fact, the EU has only recently started using the term 'cybersecurity' in its policy documents (e.g., communications, reflection papers). The adoption of a comprehensive EU Cybersecurity Strategy in 2013[48] can be considered to be the tipping point, triggering **the increased use of the term in EU policy documents** (e.g., in 2016 Communication 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry').

Nevertheless, in **measures** addressed **to the Member States**, EU institutions appear to be reluctant to use this term. That is the case, for example, of the EU adopted 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* (NIS Directive).[49] The NIS Directive lays down obligations for all Member States to adopt certain measures (e.g., national strategies on the security of network and information systems) that would allow developing a culture of security across industries and sectors which rely on the use of information communication technologies. Within the context of this Directive, '***security of network and information*** **systems**' is regarded as '*the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems*'.[50] This definition seems to align the conception reflected in the EU Cybersecurity Strategy, where the underlying objective of cyberse-

[44] For example, European Commission, Directorate-General for Communication Networks, Content and Technology, A concept paper on digitisation, employability and inclusiveness: the role of Europe, May 2017.
[45] European Communication, Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All, Brussels, 10.5.2017, COM(2017) 228 final, 13.
[46] According to Regulation (EU) No 526/2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, the assessment of ENISA mandate is carried out every 5 years (Article 24.3). In preparation for the next revision scheduled for June 2018, the European Commission has launched a public consultation in January 2017.
[47] European Commission, Reflection Paper on the Future of European Defence, June 2017.
[48] European Commission and High Representative of the EU for Foreign Affairs and Security Policy (2013), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final.
[49] Emphasis added by the authors.
[50] NIS Directive, Article 4(2).

curity is considered to be the preservation of '*the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein*'.[51] Nonetheless, the NIS Directive formally addresses 'security of information systems and networks', and not cybersecurity.

The **ambiguity embedded** in the term '**cybersecurity**' allows for the term to be invoked **across different policy areas** described in sections 2.1 and 2.2. While this is not problematic in itself, the fragmented approach may not be cost-efficient.[52]

3.2 Cooperation of Stakeholders

Combating **cybersecurity threats** and risks is a multi-disciplinary matter that requires expertise and cooperation of stakeholders within different domains, such as IT, psychology, law, education, and policy fields. **Cooperation challenges** may thus emerge **at different levels**. A good understanding of the roles of different actors and institutions assigned by law as well as those embedded in the EU governance structure can explain why tensions arise between them during the policy creation process. This in turn, can provide insights about how to facilitate and strengthen cooperation between different stakeholders.

3.2.1 Cooperation of EU Institutions and Agencies Involved in Cybersecurity Protection

Cybersecurity is a complex issue and **several EU institutions, agencies and services share responsibility** over this area. The European Commission's Directorate General (DG) for Communications Networks, Content & Technology (DG CONNECT) carries the main responsibility for implementing the policies that facilitate the creation of a Digital Single Market, thus encompassing cybersecurity. However, other Directorate Generals, such as DG Joint Research Centre, DG for Communications Networks, Content and Technology and DG for Mobility and Transport, also develop policies that directly or indirectly contribute to cybersecurity regulation. With more policy areas increasingly relying on ICT, the number of DGs that address issues related to cybersecurity has been growing. To date the cooperation between the DGs on cybersecurity affairs is often based on rigid internal communication rules rather than informal practices.

Regulatory measures, such as EU-wide legislation on cybersecurity, proposed by the European Commission, are negotiated between the European Parliament and the Council. Table 2 lists EU agencies and bodies involved in the development and implementation of cybersecurity policies, at least with a consultative role.[53] Consult Annex III for additional information.

While all these actors contribute to the overall goal of ensuring a high level of network and information security within the EU by addressing cybersecurity issues in different policy areas, their **roles and responsibilities are not set in a clear governance structure**. In order to address this challenge, ENISA, in its policy paper outlining the vision of the revised EU cybersecurity strategy, proposes a governance model that could potentially facilitate the cooperation and coordination of stakeholders' effort.[54]

[51] European Commission and High Representative of the EU for Foreign Affairs and Security Policy (2013), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final, 3.
[52] ENISA, Principles and opportunities for a renewed EU cyber security strategy, ENISA contribution to the Strategy review, May 2017, 14.
[53] This figure is adapted from European Commission and High Representative of the EU for Foreign Affairs and Security Policy (2013), *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 7.2.2013 JOIN(2013) 1 final, 57.
[54] ENISA, Principles and opportunities for a renewed EU cyber security strategy, ENISA contribution to the Strategy review, May 2017, 13-14.

In NIS	In law enforcement[55]	In defence
EDPS (European Data Protection Supervisor)		
• **ENISA** (EU Agency for Network and Information Security) • **CERT-EU** (a permanent Computer Emergency Response Team for the EU institutions, agencies and bodies) • **EP3R** (European Public-Private Partnership for Resilience)	• **EC3** (the European Cybercrime Centre at Europol) • **CEPOL** (the EU Agency for Law Enforcement Training) • **Eurojust** (EU's Judicial Cooperation Unit)	• **EEAS** (European External Action Service) • **EDA** (European Defence Agency)

Table 2: *Actors involved in cybersecurity protection in the EU. NIS: Network and Information Security.*

Furthermore, **sometimes** cooperation is hindered by **colliding positions on principled issues** that stakeholders may take. For example, the Council of the EU, representing the Member States, and ENISA, an EU agency raising awareness about network and information security in society issues for citizens, consumers, enterprises and public-sector organisations in the Union, do not share a similar opinion about the use of encryption. In November 2016, the Council of the EU proposed the launch of a reflection process on the use of **encryption in the criminal justice sector**, led by the European Commission.[56] Issues related to the use of encryption as well as its possible regulation were then further addressed in a Council meeting in November 2016. The preparatory note for the meeting underscored that '*the use of encryption deprives law enforcement of crucial evidential opportunities, especially given the fact that it is no longer restricted to desktop computers but increasingly available on mobile devices and many commercially available communication platforms have now encryption by-default (increasingly by way of end-to-end encryption leading to situations where services are not interceptable).*'[57] While recognising '*the need to address both the technical and legal (criminal justice) aspects of the issue [of encryption] and to focus future work on practical solutions that would facilitate law enforcement work without undermining encryption as such and the protection of citizens' privacy*', **the Council of the EU** reiterated that **a careful balance** should be struck between **the needs of law enforcement and citizens' rights**.[58]

ENISA seems to hold a different opinion on the regulation of encryption. In its opinion paper on the subject, ENISA concluded that **weakening encryption to enable lawful interception is not an optimal approach**. ENISA noted that as a result of weakening encryption, security of digital signatures and many other applications would be undermined. ENISA invited to carry out further benefits and risks analysis, as well as a more in-depth exploration of alternatives before taking any legislative actions.[59] Similarly, the European Data Protection Supervisor (EDPS), an independent data protection authority monitoring the processing of personal data by EU institutions and bodies, has on several occasions reiterated that

[55] Here, 'law enforcement' is to be understood in a broad meaning that includes any entity that contributes to law enforcement.
[56] Cf. Note 14711/16 from the Council of the European Union Presidency to the Permanent Representatives Committee/Council on the subject title '*Encryption: Challenges for criminal justice in relation to the use of encryption - future steps - progress report*', Brussels November 23rd 2016, 7.
[57] Council of the EU, Presidency Progress report: Encryption: Challenges for criminal justice in relation to the use of encryption - future steps, LIMITE CYBER 137, JAI 976, 14711/16, Brussels, 23 November 2016.
[58] Outcome of the 3508th Council meeting, document 15391/16 and press release 67 by the Justice and Home Affairs department, section '*Criminal justice in Cyberspace*', Brussels, 8th and 9th December 2016, 7.
[59] European Union Agency for Network and Information Security, '*ENISA's Opinion Paper on Encryption - Strong Encryption Safeguards our Digital Identity*', December 2016, 5.

installing backdoors to devices or encryption schemas in order to identify criminals and terrorists would impinge on security of all devices and applications that include encryption.[60]

In any case, EU institutions and bodies working on different aspects of cybersecurity policy aim at cultivating their cooperation through both formal and informal ways, such as networks of specialised experts, conferences and multi-stakeholder gatherings.[61]

3.2.2 Cooperation between National Authorities within the individual Member States, as well as within the EU

While the EU Cybersecurity Strategy calls for a comprehensive approach towards cybersecurity protection, three pillars constitute different legal frameworks tackling cybersecurity capability. These include the network and information systems, law enforcement, and defence.[62] This approach has developed as a result of previous policy documents which recognised that '*effective policy making needs a clear understanding of the nature and extent of the challenges*' brought by technologies and which to this end suggested '*a three-pronged*' approach that would include 1) specific network and information security measures, 2) the regulatory framework for electronic communications (which includes privacy and data protection issues), and 3) the regulatory framework for the fight against cybercrime.[63]

Consequently, there are numerous entities that are responsible for enforcing or monitoring compliance with different frameworks at national level. The EU encourages cooperation between these entities responsible for various dimensions of cybersecurity. However, in practice cooperation extends to their counterparts in other countries through various cooperation groups (e.g., Article 29 Working Party, the Body of European Regulators for Electronic Communications (BEREC)). In some cases, entities and regulators having responsibilities over different areas of cybersecurity within a country do not have effective communication practices and legislative bases governing their information exchange put in place (e.g., between CERTs and law enforcement authorities). In this regard, the mandatory requirement to adopt national strategies on the security of network and information systems, introduced by the NIS Directive, is very timely.[64] It aims at ensuring that Member States clarify their cybersecurity governance framework and define roles and responsibilities of stakeholders in the public and private sectors. The attribution of clear responsibilities and roles to each entity is considered to facilitate cooperation.

The European Criminal Policy Initiative, led by a group of criminal law scholars, is an example of bottom-up development, which seeks to clarify roles of law enforcement authorities. In 2013, it published a manifesto concerning '*the laws of criminal procedure and mutual legal assistance, which recently have increasingly been shaped by Union legislation*'. [65] The manifesto insisted on adhering to the highest standards of the rule of law and protection of fundamental rights within the scope of laws governing

[60] See, EDPS, Guidance on Security Measures for Personal Data Processing Article 22 of Regulation 45/2001, and EDPS, Opinion 8/2015 Dissemination and use of intrusive surveillance technologies.
[61] For example, Europol organized a conference on privacy in the digital age of encryption and anonymity online in 2016. This conference brought together stakeholders from various backgrounds, including law enforcement agencies, as well as representatives of the legislator, justice, private parties, academia, NGOs and any other experts willing to share their perspective in order to contribute to effectively striking the right balance between freedom and security. ENISA organizes the Annual Privacy Forum, which provides a platform for exchange of ideas ranging from policy priorities to scientific developments, also see: European Commission, Commission Staff Working document 'Comprehensive Assessment of EU Security Policy accompanying the document Communication to the European Parliament, the European Council and the Council: Ninth progress report towards an effective and genuine Security Union' (Part 1), Brussels, 26.7.2017 SWD(2017) 278 final, 70.
[62] European Commission and High Representative of the EU for Foreign Affairs and Security Policy (2013), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final, 4.
[63] European Commission, Communication - A strategy for a Secure Information Society - 'Dialogue, partnership and empowerment' {SEC(2006) 656} /* COM/2006/0251 final, 8.
[64] NIS Directive, Article 7.
[65] European Criminal Policy Initiative, 'Manifesto II'.

criminal procedure, even though in this area of law legislature seeks to balance interests of states, societies and individuals.[66] It put forward six demands for the EU legislator: 1) limitation of mutual recognition[67], 2) balance of the European criminal proceeding[68]; 3) respect for the principle of legality and judicial principles in European criminal proceedings[69]; 4) preservation of coherence; 5) observance of the principle of subsidiarity[70]; 6) compensation of deficits in the European criminal proceedings.[71] While little action has been taken in response to these demands, discussion on the EU role within the area of freedom, security and justice is still ongoing.[72]

3.3 Securitization of EU Values and Interests

The observation that '*information revolution makes security and increasingly important concern in all sectors of society*'[73] withstands the test of time and accurately reflects the current debates within the EU.[74] In the reflection paper on the future of cybersecurity regulation, the EC emphasises the need to protect European values and interests against new types of threats.[75] In order to improve the competitiveness and security of the EU, the reflection paper considers three scenarios (i.e., Security and Defence Cooperation, Shared Security and Defence, Common Defence and Security) which would allow pooling Member States' industrial and technical resources. Within the scope of this document, the EC questions EU competencies in the field of cybersecurity and considers ways to extend them beyond the limits of Digital Single Market. Cybersecurity becomes intertwined with objectives of a Security and Defence Union and it is suggested that deeper integration, in particular the creation of a Common Defence Security, would improve cybersecurity resilience both at national and EU levels. It is also argued that deeper integration scenario would allow for '*Europe […] to deploy detection and offensive cyber-capabilities', which could be used in case of 'cyber-attacks or external interference in Member States' democratic processes'*.[76]

The European Commission's rhetoric in the recent policy documents is somewhat biased as it insists on the need for more cooperation and coordination of programmes concerning the interoperability of information systems for security, border and migration management.[77] For example, the European Commission in one of its recent documents refers to '*the global cyberattack using ransomware'* (known as WannaCry) as a case demonstrating the need for expansion of EU actions, and thus competences, within the cybersecurity domain.[78] In the other policy document, the European Commission relies on statistics about ransomware from the United States in order to strengthen its claim about the potential risks of cyberattacks for business, economy and democracy in the EU; '*wider instruments for European solidarity*

[66] Ibid., 430.
[67] Through the rights of the individual (suspect, victim or third person), through the national identity and *ordre public* (public policy) of the Member States, and through the principle of proportionality.
[68] Warning against a possible shift in power solely in favour of the prosecution, they suggest creating supranational institutions that strengthen the position of the affected individuals.
[69] There is a need for a clear set of rules governing which Member States may exercise criminal jurisdiction.
[70] EU action may only be taken on the condition that the goal pursued a) cannot be reached as effectively by measures taken at the national level, and b) due to its nature or scope can be better achieved at Union level.
[71] Safety mechanisms should include compensation measures to ensure that the first five demands are met.
[72] European Commission, Reflection Paper on the Future of European Defence, June 2017.
[73] Eriksson, J., Giacomello, G., 'The information Revolution, Security and international Relations; (IR)relevant theory?' International Political Science Review Vol. 27, No. 3, 2006, 221-244.
[74] European Commission, Reflection Paper on the Future of European Defence, June 2017, 6.
[75] Ibid., 6.
[76] Ibid., 14-15.
[77] Idem.
[78] European Commission, Communication on Seventh progress report towards an effective and genuine Security Union, 16.5.2017 COM(2017) 261 final, 2.

and mutual assistance' in the field of cybersecurity could address these risks.[79] This far stretched rhetoric contradicts the rationale of EU better regulation policy which should be driven by the '*best available evidence*' and the involvement of stakeholders.[80] Public statements made by some EU officials hint that the European Commission could have taken a different approach in response to the increasing number of cyberattacks and cyberthreats. For example, the Assistant EDPS suggested that if appropriate security measures, required under data protection law, had been implemented, the recent attacks could have been prevented.[81] This observation suggests that in response to cyberthreats, the European Commission could have emphasised the need for better implementation of requirements stemming from EU data protection framework rather than on the need for stronger cooperation mechanisms.

Finally, the fight against cybercrime constitutes an essential part of cybersecurity, although it addresses a limited subset of threats. As cybercrime is endangering our societies from the online world, criminal justice contributes to the protection of our assets and uphold our values in the cyberspace. Cybercrime is inseparable from criminal law since the latter defines it. However, the fight against cybercrime is not merely a legal issue. The THOR concept presents four dimensions of the problem: (T)echnical, (H)uman, (O)rganisational, and (R)egulatory, the regulatory dimension being 'related to law provisioning, standardisation and forensics'.[82] For more information on issues concerning the area of freedom, security and justice, consult Annex III of this White Paper.

[79] European Communication, Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All, Brussels, 10.5.2017, COM(2017) 228 final,12.
[80] European Commission, Commission Staff Working Document, Better Regulation Guidelines, Strasbourg, 19.5.2015 SWD(2015) 111 final, 5.
[81] Wiewiórowski Wojciech, Privacy, security and technology: the Annual Privacy Forum 2017, notes available at: https://edps.europa.eu/press-publications/press-news/blog/privacy-security-and-technology-annual-privacy-forum-2017_en.
[82] Choraś and Kozik, *CAMINO Roadmap*, 7.

4. Controversies over Cybersecurity Regulation

4.1 Defining Controversies

Debates on the regulation of **cybersecurity in the EU** are marked by a series of crucial **controversies**, the number of which is steadily increasing, as cybersecurity impacts a wider range of policy domains. Similarly to controversies in other fields, those in this area imply that there is '*a lot of disagreement or argument about something, usually because* [the issue at stake] *affects or is important to many people*'.[83] Indeed, cybersecurity is of great importance for **stakeholders representing multiple viewpoints**, as well as **industries that hold particular perspectives** and interests. Currently, ten controversies stand out for their role in shaping debates over cybersecurity regulation in the EU. For more controversies concerning EU cybersecurity law and specific literature references, consult Annex III on criminal justice and Annex IV on privacy and personal data protection law.

4.1.1 Fundamental Rights as Drivers for EU Regulation?

Many EU policy documents in the cybersecurity domain recognise that any measures taken with respect to the protection of EU citizens, society as well as information systems and infrastructure have to be developed '*in accordance with the commitment of the European Union to respect fundamental human rights*'.[84] Since the entry into force of the Lisbon Treaty, there has been a**n ever greater emphasis on** such imperative of adhering to **fundamental rights**, in the **EU policy documents, legislation and bilateral agreements** that facilitate cooperation in the law enforcement area.

For example, the NIS Directive in its Recital 75 notes that the '*Directive respects the fundamental rights, and observes the principles, recognised by the Charter of Fundamental Rights of the European Union (EU Charter), in particular the right to respect for private life and communications, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy before a court and the right to be heard*',[85] before emphasising that obligations imposed by the Directive should be implemented in accordance with the aforementioned rights and principles. Then, the European Commission in its proposal for the ePrivacy Regulation, updating the rules governing the processing of data through electronic communication networks, proposed extending the scope of confidentiality obligations, which are at the core of the EU fundamental right to privacy. In particular, the European Commission proposed that the ePrivacy Regulation applies to the so-called 'over the top' services (OTTs), such as Voice over IP, and communications services that are ancillary to another service, such as a chat on a gaming platform.[86]

Fundamental rights and principles enshrined in **the EU Charter**, however, must be considered only to the extent where the EU law is applicable. Article 51(1) of the EU Charter specifies that its provisions are addressed to EU institutions, bodies, offices and agencies and to the Member States only when they

[83] Cambridge Dictionary, http://dictionary.cambridge.org/dictionary/english/controversy.
[84] European Commission, Communication, 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime', COM(2000) 890, 2; see also: European Commission, Communication, The Digital Agenda for Europe - Driving European growth digitally, COM(2012) 784 final, 12; Council of the EU, The Stockholm Program: An open and secure Europe serving the citizen, 17024/09, 4.
[85] Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.
[86] European Commission, 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), Recital 11.

are implementing Union law.[87] The latter is broadly interpreted by the CJEU. In *Aklagaren v Hans Akerberg Fransson*, the CJEU inferred that provisions of the EU Charter apply in view of Treaty obligations and no particular EU measure needs to be implemented.[88] The CJEU emphasised that *'[t]he applicability of European Union law entails applicability of the fundamental rights guaranteed by the Charter*'.[89] Nevertheless, in a number of instances compliance with fundamental rights requirements by the EU legislator has been not only questioned, by actually refuted by the judiciary.

For example, the current legal set up allowed to successfully challenge on fundamental rights grounds Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (the Data Retention Directive) at the Court of Justice of the EU. The Data Retention Directive was annulled by the Grand Chamber of the Court on the grounds that the blanket collection of communication data, in particular traffic and location, by providers of communication providers was not proportionate (i.e., excessive), and therefore constituted an infringement of the rights privacy and protection of personal data of individuals that are enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the EU.[90] This decision did however not automatically annul Member States' laws implementing the Data Retention Directive.

The Court of Justice of the EU (CJEU) Opinion 1/15 concerning the draft agreement between the European Union and Canada on the transfer of Passenger Name Record is also an illustrative example highlighting the importance of adherence to the fundamental rights recognised by the EU.[91] In the Opinion the CJEU concluded that the envisaged agreement might not be concluded in its current form because rules governing the transfer of PNR data from the EU to Canada entail an interference with the fundamental rights to respect for private life and the protection of personal data.

These examples demonstrate that values stemming from the EU Charter play an important role in the EU regulatory approach in the cybersecurity domain, even though they are contested by the EU institutions. It is suggested that a strong emphasis put on the protection and promotion of fundamental rights form a unique and distinctive EU approach to cybersecurity.[92] This approach is often challenged during multilateral and bilateral negotiations with international organisations and EU strategic partners for cooperation on cyber policy.[93] For protection of fundamental rights to become an established principle in the cybersecurity domain, the EU has to consistently advocate for it in its internal and external measures.

4.1.2 Regulation through Individual Risk Identification and Proactive Action

Recent regulatory measures, such as the GDPR and NIS Directive, impose requirements aiming at improving cybersecurity. The basic principle here is that the ones responsible for the operations must take appropriate security measures. For example, the NIS Directive stipulates that operators of essential services must '*take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations'*.[94] In particular, the operators of essential services should also '*take appropriate measures to prevent and*

[87] Consolidated Version of the Treaty on European Union and the Treaty on the Functioning of the European Union (2010/C 83/01); The EU Charter, Article 51 (1).
[88] Court of Justice of the European Union, *Aklagaren v Hans Akerberg Fransson* (C-617/10) 23 February 2013, § 30.
[89] Idem., § 28.
[90] Court of Justice of the European Union, Joined Cases *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General* (C-293/12) *and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others* (C-594/12), 8 April 2014.
[91] Court of Justice of the European Union, Opinion 1/15 Draft agreement between Canada and the European Union — Transfer of Passenger Name Record data from the European Union to Canada, 26 July 2017.
[92] Darmois, E. and Schméder, G., Cybersecurity: a case for a European approach, Paper commissioned by the Human Security Study Group SiT/WP/11/16, 19.
[93] Ibid.
[94] NIS Directive, Article 14.1.

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'. [95] In a similar vein, the GDPR requires data controllers and processors to *'implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*'.[96]

This approach is controversial because it **relies on responsible parties** identifying the risk and acting upon it **independently**, with no interference of regulators. However, **measuring risk** is contextual and is considered to be a knowledge intensive process.[97] Hildebrandt and Tielemans suggest that the use of the word 'appropriate' relates to the contextual and dynamic nature of such measures.[98] In practice, this means that what is appropriate changes and depends on the identified risk. Depending on the applicable framework, **a party responsible for implementing appropriate measures**, (e.g., controllers, processors or providers of essential services) **carries a duty to identify risks** associated with their activities or business, such as the provision of services. But how accurate are these entities in their risk identification processes? These entities are also awarded **a wide discretion** to determine appropriate technical and organisational measures that are most appropriate in response to these risks. It should be noted that appropriate measures include not only technical solutions but also organizational practices and policies.

Additionally, both the GDPR and NIS Directive require a party responsible for the implementing appropriate measures to consider '**the state of the art**'. 'The state of the art' is as such **a dynamic concept** and requires the responsible entities or the ones designing services for them to consider the most recent developments and knowledge associated with technologies that are used. Gathering knowledge and information about the 'state of the art' requires controllers **to keep up to speed with** various **developments in fields concerning standardisation** (e.g., regional or international standards), technology (e.g., software and hardware solutions), **cyber threats**, and **research**. Invoking the concept of 'the state of the art' may be indicative of the rapidly changing security landscape. However, while this obliges responsible parties (mostly IT industry actors) to continuously learn about the recent trends and best practices concerning security measures that are available in the market, it neither mandates the use of any specific technologies, nor it requires to spend a certain percentage of the investment on 'appropriate' organisational and technical measures. Some suggest that this amount should reach about 37 % of the expected loss that could result from a cybersecurity breach, but in practice, the exact amount that is invested in security measures depends on the nature, scale, context of the processing as well as on information sets that are going to be processed.[99]

4.1.3 Attribution of Roles to Different Stakeholders

One of the key challenges of cybersecurity regulation is **to impose** the right **obligations on the right actors**. Current regulation of data protection by design focuses exclusively on data controllers (i.e., entities defining the means of the processing of personal data), which may address only part of the problems in the area, as this obligation to implement data protection by design does not extend to the actual developers of technology or service providers. Recital 78 reveals some of the hesitations of the legislator, mentioning not only controllers and processors but also the producers of the products, services and applications. In particular, the Recital encourages the latter '*to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection*

[95] Ibid., Article 14.2.
[96] GDPR, Article 32.
[97] Black J., 'The role of risk in regulatory processes' in R. Baldwin, M. Lodge and M. Cave *Oxford Handbook of Regulation,* OUP, 2010.
[98] Hildebrandt, M., Tielemans, L., 'Data protection by design and technology neutral law', Computer law & Security Review 29 (2013) 509-521.
[99] Gordon, L.A., Loeb, M.P., Zhou, L., Investing in Cybersecurity: Insights from the Gordon-Loeb Model, Journal of Information Security Vol.7 No.2, 2016.

obligations'.[100] While recognizing value of this Recital, it should be noted that the actual software developers or producers of hardware, unless they are data controllers or processors, are not subjected to legal obligations foreseen in the EU data protection framework. The debate within the field of data protection over who should be responsible for ensuring rights of individuals in the online environment is still ongoing in the EU. Discussions concerning the proposed ePrivacy Regulation also confirm that this is an unresolved issue.[101]

Likewise, **the EU liability framework in many cases may favour software developers**. While software is not explicitly included in the scope of the Product Liability Directive, it is acknowledged that for the purposes of product liability software should be perceived as a product.[102] According to the Product Liability Directive, which has been transposed into national laws, any person in the supply chain can be held liable and requested to compensate victims for any personal injury or damage caused to private property caused wholly or in part by a defect of a product. In such cases the plaintiff does not have to prove negligence on the part of the producer, but only that it is was defective and the damage occurred because there was causality between the defect and damage.[103] This in practice means that the EU has opted in for a strict liability regime for which no proof of fault is necessary. At the same time, it should be noted that in circumstances where a product leads to a pure economic loss or infringement of individuals' right, the strict liability regime may not be invoked as the damage should occur to a person or to a private property. Furthermore, the Product Liability Directive in Article 7 foresees that there are several situations in which the producer's liability can be avoided.[104] The European Parliament has recently noted that in the context of Internet of Things (IoT), '***tightening up liability regimes***' would be **desirable** as it could '*lead to a better quality of products and a more secure environment*'.[105]

It is also argued that a **new approach to the liability framework** that could provide individuals with comprehensive and meaningful protection of their security, including the protection of their personal data, is needed.[106] The new approach, proposed by Daley, would require to 1) balance ex ante incentives to invest in security with ex post liability 2) incentivize software developers to publicly disclose source code, 3) promote trust and public confidence in embedded systems. [107] It seems that this approach, though being controversial, could help to develop '*high-quality, affordable, interoperable and trustworthy cybersecurity products*' that EC has called for in June 2017.[108]

[100] GDPR, Recital 78.
[101] EDPS, Opinion 6/2017 EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation).
[102] Alheit, K., 'The applicability of the EU Product Liability Directive to Software', Comparative and International Law Journal of Southern Africa, Volume 34, Issue 2, Jul 2001, 194.
[103] Ibid., 197-199.
[104] Product liability in the European Union, A report for the European Commission, February 2003 European Commission Study MARKT/2001/11/D, Contract No. ETD/2001/B5-3001/D/76: (a) that he did not put the product into circulation; or (b) that, having regard to the circumstances, it is probable that the defect which caused the damage did not exist at the time when the product was put into circulation by him or that this defect came into being afterwards; or (c) that the product was neither manufactured by him for sale or any form of distribution for economic purpose nor manufactured or distributed by him in the course of his business; or (d) that the defect is due to compliance of the product with mandatory regulations issued by the public authorities; or (e) that the state of scientific and technical knowledge at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered; or (f) in the case of a manufacturer of a component, that the defect is attributable to the design of the product in which the component has been fitted or to the instructions given by the manufacturer of the product.
[105] European Parliament, Report on the fight against cybercrime, 2017/2068, A motion for a European Parliament Resolution, 13.
[106] Daley, J., 'Insecure software is eating the world: Promoting cybersecurity in an age of ubiquitous software-embedded systems', 19 The Stanford Technology Law Review 533 (2016), 533-546.
[107] Idem, 541.
[108] Speech by Vice-President Ansip at the Chatham House annual cyber conference: Evolving norms, improving harmonisation and building resilience, June 26, 2017.

4.1.4 A Number of Individuals' Rights Grows despite the Shortfall in Digital Skills

Even though the 2015 Special Eurobarometer on Data Protection suggests that nine out of ten Europeans appear to consider the protection of their personal information to be important, the great majority of the EU citizens lack digital literacy that would enable enforcement of their rights. More than 60 % of the respondents are not aware about national authorities that could help them to enforce their rights. Even though this number has been reducing, it should raise questions about the actual value of expanding the number of data subjects' rights in the GDPR. Additionally, the recent study (Digital Economy and Society Index) shows that while 79 % of Europeans go online regularly (at least once per week), 44 % of Europeans still do not have basic digital skills.[109] Therefore, enhancing digital literacy and skills is of a particular importance in view of the existing and new rights that individuals are entitled to in the digital environment.

For example, the GDPR (Article 20) introduced the right to data portability in order to provide individuals with more control over their personal data. This right would also allow mitigating the risk of vendor lock-in. Some suggest that the right to data portability, which can be exercised by individuals, morphed out of the so called 'data ownership' debate concerning social media platforms. This right initially should have allowed individuals to move across platforms easier. In particular, it should have allowed moving, copying or transferring personal data as controllers should provide their data in '*a structured, commonly used and machine-readable format*'.[110] As Article 29 Working Party explains, this right is much broader than the existing right to data access and it is expected that it will have a significant impact on market dynamics way beyond providers of social media platforms.[111] At the same time, when being put to practice this right may expose personal data to cybersecurity risks during the transit or at the time it is at the disposal of individuals. If implemented without appropriate security measures, this right may facilitate cybercrime, in particular, social engineering and phishing attacks.

4.1.5 Understanding and Guaranteeing Controllership of Data

Controversy surrounding the debates on the notion of data controllership lays in the difficulty to attribute appropriate responsibilities for actors involved in the processing of personal data. Controllership of data may be difficult to determine and exercise due to complex data flows between and amongst the entities. For example, transparency obligations concerning notifications of data breaches and information security incidents to relevant national authorities (e.g., DPAs and CERT), may result in information exchange over which affected entities may have little knowledge and control.

The GDPR further advances debates on data controllership by 1) clarifying the accountability principle (Article 24), 2) specifying and introducing new responsibilities of data processors (Article 28), 3) introducing the notion of joint controllership and 4) introducing new data subjects' rights. The debate over the attribution of responsibility between the agents engaged in the processing of personal data. Despite regulatory attempts to clarify roles and responsibilities of each actor engaged in and affected by the processing, the debate on data controllership remains unresolved.

In principle, the determination of who is a controller responsible for a particular processing operations, must always take into account the actual circumstances of the processing and the factual influence of the entity in question.[112] Consequently, not all recipients of personal data are controllers. Rather, in cases where another entity determines purposes and means of the processing, the recipient could be a processor. Nonetheless both, controller(s) and processor(s) are obliged by the GDPR to ensure the protection of personal information. In case of a possible non-compliance with the GDPR requirements, the affected data subject or a not-for-profit body, organisation or association mandated by a data subject

[109] Digital Economy and Society Index, Results of the study are available at: https://ec.europa.eu/digital-single-market/en/desi.
[110] GDPR, Article 20.1.
[111] Article 29 Working Party, Guidelines on the right to data portability, April 2017.
[112] Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", February 2010, 11.

or the Member State (Article 80) can turn to a supervisory authority in order to hold controller(s) and the processor(s) liable. In case an infringement is determined, the data subject can demand compensation for material or non-material damage suffered (Article 82).

Debates over data controllership should not be confused with debates on data ownership and data localisation initiatives, which gained fresh prominence with Snowden revelations. The data ownership debate questions 'Who does own the data?' and considers possibilities to monetize personal data. This debate is shaped by the list of EU regulatory measures governing trade secrecy, intellectual property, data protection and consumer protection rights.[113] Whereas data localisation initiatives typically build on the ideas that information security and better protection of individuals' fundamental right to data protection could be attained if data are not sent outside the EU (or a particular country).[114] This approach can create new opportunities for businesses adhering to the EU data protection standards and operating on the EU soil. At the same time, it may have a negative impact on EU attempts to cooperate with third countries on cybersecurity affairs.

4.1.6 Enforcement of copyright

Challenges of **copyright enforcement online** is an illustrative example of controversies brought by digitisation to traditional forms of **infringements**. While cultural, innovation and creative sectors continue to rely on protection offered by intellectual property rights in order to protect their creative work as well as financial investments, the copyright enforcement online has become a part of the wider debate on the Internet governance. Copyright protection on the Internet is a huge challenge: how to enforce intellectual property rights (IPRs) when their infringements are so widespread? Can and under what conditions intermediaries and Internet Service Providers (ISPs) be held liable for their users' behaviour?

Whereas some would like to reduce or even abolish copyright, rights holders strive to strengthen copyright protection and enforce it by all means, including through the criminal law. '[*D]ifficult questions arise as to the correct balance to be achieved between protecting the rights of the right holder, on the one hand, and protecting other interests such as the internal market or individual rights, such as freedom of information, on the other.[…] In addition, … copyright protection in the digital age cannot be divorced from matters such as 'Internet freedom' not least because there is considerable potential for obligations to be placed on Internet subscribers or Internet service provider (ISPs) to ensure that Internet connections are not used to infringe intellectual property. […] In short, as soon as the focus moves away from commercial activities and towards the practices of individuals, the criminalisation of copyright infringement becomes controversial.*'[115]

The CJEU on several occasions engaged in the **balancing exercise** of **economic interests**, in particular the right to protection of **intellectual property rights**, and **human rights** in the online environment. In the case of *Scarlet Extended*, the CJEU concluded that an obligation for ISPs to install filtering software in order to conduct **blanket searches** for unlawful content is **in breach** of both EU **data protection rules** and **freedom of expression** online as such software might have blocked lawful communication.[116] The same was confirmed in *SABAM v. Netlog NV*, in which the CJEU found that '*owners of social networking sites cannot be obliged to install general filtering systems to cover all their users, even if these filtering systems would be effective in preventing the unlawful use of copyrighted material*'.[117] In both cases the CJEU favoured data protection rules, the freedom to conduct business and the freedom to receive or impart information and framed **intellectual property rights** in a **narrow fashion**.[118]

[113] European Commission, Legal study on ownership and access to data, 2016, 978-92-79-62181-9.
[114] Kuner, C., 'Data Nationalism and Its Discontents', 2014, 64 Emory Law Journal 2089-2098.
[115] Ibid., 119.
[116] Court of Justice of the European Union*, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL* (SABAM) (C-70/10), 24 November 2011.
[117] Benedek, W., Kettemann, M.C., Freedom of expression and the Internet, Council of Europe, 15 Jan 2014, 76. Also see: Court of Justice of the European Union, *SABAM v Netlog NV* (C-360/10), 16 February 2012.
[118] Ibid.

4.1.7 Regulating Online Content

Freedom to opinion and **freedom to expression** are often stifled, even though the internet is predominantly considered to be an empowering medium that allows individuals to exercise their fundamental rights and freedoms. On frequent basis, actions of diverse stakeholders engaged in the internet governance undermine the enjoyment of freedom to opinion and freedom to expression. **Internet content suppression** (ICS) is a key form in which infringements and interferences with the two freedoms manifest. Ever more sophisticated technologies ease the implementation of online content regulation measures, such as ICS. Nonetheless, *'to be in compliance with human rights, ICS requires careful balancing of public and private interests with freedom of expression'*[119]. Consequently, content regulation online is a controversial subject.[120] '*The determination of what constitutes 'criminal' as opposed to 'lawful' content depends to a large extent on the political and cultural context in which issues such as censorship, freedom of expression and more broadly the relationship between the individual and the government are determined*.'[121] For more information about controversies surrounding the term 'cybercrime', consult Annex III, section 2 and its subsections.

EU policy distinguishes between harmful content and illegal content. '*Illegal content is considered obviously and universally unlawful, whereas the decision about whether content is 'harmful' or not is considered to depend on 'cultural differences*''.[122] But even illegal content stirs controversy. '*Some offences, notably those relating to child pornography, are widely accepted as necessary even though questions remain as to their scope, while others, such as some of the provisions on terrorist offences are the subject of considerable controversy both as regards their desirability in the first place and their extent*.'[123] *Directive 2011/93/EU* defines a child as any person below the age of 18 years[124], although young people under 18 already have sexual consent in all EU countries except Malta. Child pornography includes '*not only pornographic material involving actual children, but also pornographic material involving adults who look like children (youthful adult pornography) and computer-generated pornographic material involving children, although not created using any actual children (virtual-child pornography).*'[125] Some argue that '*these broad provisions, which seem to test the boundaries of the criminal law, will nevertheless prove difficult to reconcile with constitutionally protected notions of free speech and the presumption of innocence. (…) 'The emphasis shifted from protecting children from harm to attacking possession itself.*'[126] Others question the legal certainty of youthful-adult pornography: *'[w]hether or not a person of age appears as a minor cannot be described legally. (…) This criterion will not lead to foreseeable results and is not suitable for the use in criminal law provisions.*'[127]

4.1.8 Regulating Encryption

The issue of **encryption** has been discussed in different contexts in the EU. Encryption is considered to be one of the **security measures** within the scope of **EU data protection framework**[128] and it is **widely embraced** by academics[129] and the prominent actors within the cybersecurity domain, such as ENISA and EDPS.[130] However, Member States, especially the ones that have recently suffered terrorist attacks,

[119] De Hert, P., Jasmontaite, L., Internet Content Suppression, in De Gruyter et al., *Culture and Human Rights: The Wroclaw Commentaries,* 2016, 76.
[120] Summers et al., *The Emergence of EU Criminal Law* Cf. Ibid., 156–98.
[121] Ibid., 156.
[122] Ibid., 162.
[123] Ibid., 168. Again, regulation in these areas can be viewed negatively as limiting the freedom of speech.
[124] In accordance with the Lanzarote Convention.
[125] Summers et al., *The Emergence of EU Criminal Law*, 179.
[126] Ibid., 181.
[127] European Criminal Policy Initiative, 'Manifesto I', 713.
[128] GDPR, 32.1(a).
[129] High Level Group of Scientific Advisors, Cybersecurity in the European Digital Single Market. SAM, Scientific Opinion No. 2/2017 March 2017, 31.
[130] European Union Agency for Network and Information Security, '*ENISA's Opinion Paper on Encryption - Strong Encryption Safeguards our Digital Identity*', December 2016, 5.

take a different view on encryption in the context of the fight against crime.[131] The Council of the EU, driven by Member States' initiatives ran a questionnaire on '*obstacles faced by law enforcement authorities when gathering or securing encrypted e-evidence for the purposes of criminal proceedings*' in 2016.[132] This questionnaire had to facilitate further discussions on the common European approach on the use of encryption. It found that '*encryption is encountered often or almost always in the context of criminal investigations*' and that encryption challenges are encountered '*both with regard to online (in the form of encrypted emails or other forms of e-communication and/or commercial applications such as Facebook, Skype, WhatsApp or Telegram) and offline encryption (most often criminal investigation involving encrypted digital devices and encrypting applications)*'.[133] In order to overcome such challenges, law enforcement and intelligence services advocate for the creation of means allowing to circumvent security solutions that cryptography provides. This in essence would require the development of a backdoor, which would allow for a third party to '*have a mechanism to independently and without the knowledge of the sending or receiving party decrypt the communication*'. [134] In response to this call, ENISA noted that '*limiting the use of cryptographic tools will create vulnerabilities that can in turn be used by terrorists and criminals, and lower trust in electronic services, which will eventually damage industry and civil society in the EU*'.[135] It also encouraged exploration of other procedural approaches that would facilitate the judicial process.[136]

The intense discussions on encryption regulation were put on halt for a few months but they resurfaced with the European Parliament's amendments to a draft ePrivacy Regulation. One of the proposed amendments requires that '*in order to safeguard security and integrity of networks and services, the use of end-to-end encryption should be promoted and, where necessary, be mandatory in accordance with the principles of security and privacy by design'.* [137] If adopted during the legislative negotiation processes, this provision would also forbid Member States from imposing *'any obligation on encryption providers, on providers of electronic communications services or on any other organisations (at any level of the supply chain) that would result in the weakening of the security of their networks and services, such as the creation or facilitation of "backdoors".'*[138] It remains to be seen how this debate unfolds in the near future and whether ENISA's and EDPS' warning that installing backdoors to devices or encryption schemas in order to identify criminals and terrorists would impinge on security of all devices and applications that include encryption, is taken into consideration. [139]

4.1.9 Permissibility of Massive and Generalised Surveillance of Individuals

Another key controversy in the area of cybersecurity is the extent to which the massive and generalised surveillance of individuals is permissible, and more specifically whether it is compatible with the requirements of the EU Charter of Fundamental Rights. The EU has launched several large-scale IT systems, namely, the second generation Schengen Information System (SIS II), the Customs Information System (CIS), the Visa Information System (VIS), the Internal Market Information System (IMI), and a large da-

[131] Council of the EU, Note from presidency to delegations Brussels: Encryption of data, 12368/16 LIMITE CYBER 102, 20 September 2016, 1.
[132] Ibid.
[133] Council of the EU, Presidency Progress report: Encryption: Challenges for criminal justice in relation to the use of encryption - future steps, LIMITE CYBER 137, JAI 976, 14711/16, Brussels, 23 November 2016, 3.
[134] European Union Agency for Network and Information Security, ENISA's Opinion Paper on Encryption Strong Encryption Safeguards our Digital Identity, December 2016, 7.
[135] Ibid, 16.
[136] Ibid.
[137] European Parliament, Draft Report by Marju Lauristin (PE606.011v01-00), 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), Amendment 276, Sophia in 't Veld, Angelika Mlinar, Proposal for a regulation Recital 26 a (new).
[138] Ibid.
[139] See, EDPS, Guidance on Security Measures for Personal Data Processing Article 22 of Regulation 45/2001, and EDPS, Opinion 8/2015 Dissemination and use of intrusive surveillance technologies.

tabase of fingerprints of applicants for asylum and irregular immigrants found within the EU (Eurodac).[140] All of these systems fall under EDPS supervision and they have separate legal bases, content and architecture of their IT systems. The massive processing of information about individuals is a distinctive feature of these large-scale IT systems – understood in a broad manner as EU security measures. It has been suggested that EU attempts to strengthen external border controls and the development of these large scale IT systems allowed the EU to move from 'border control' to 'border security', with the latter being directly linked to counterterrorism.[141] Border-related security initiatives have been considered to intensify surveillance in a manner that is at odds with the concept of the EU as a borderless area, leading to the paradoxical situation of an area without frontiers but with more controls, in which the abolition of (internal) borders seems to prompt the emergence of new forms of control.[142] The EU has recently revised legal frameworks governing its large scale IT systems.

However, not all surveillance systems are acceptable in the EU. In this sense, the Data Retention Directive concerning the retention of traffic and location data of all subscribers for the purpose of investigation, detection and prosecution of serious crime can be recalled. The Directive required communications providers to store metadata (i.e., information about their source, destination, date, time and location) for the period of time ranging from six months to two years. The Directive was annulled as the CJEU took a view that it '*entails an interference with the fundamental rights of practically the entire European population because it concerns all persons and all means of electronic communication. […] [Therefore,] the EU legislature has* ***exceeded the limits*** *imposed by compliance with* ***the principle of proportionality*** *in the light of Articles 7, 8, and 52(1) of the Charter*'.[143] In a similar vein, the CJEU concluded that '*legislation* ***permitting*** *the* ***public authorities*** *to have* ***access*** *on a generalised basis to the content of electronic communications must be regarded as* ***compromising the essence of the fundamental right*** *to respect* ***for private life****, as guaranteed by Article 7 of the Charter*' in *Maximillian Schrems v Data Protection Commissioner* case that led to the annulment of the Safe Harbour Agreement allowing for the transfer of personal data to the United States.[144] The other interesting case untangling security issues form the protection of fundamental rights is *Breyer v Bundesrepublik Deutschland.* In this case, the CJEU concluded that the legitimate interest basis does not justify personal data collection of anyone who accesses a website for the purposes of security and continuous proper functioning of that website.[145]

4.1.10 Fighting Terrorism

Most of the EU's counter-terrorism measures that are legally binding, such as directives, framework decisions, decisions and international agreements, are mostly '**crisis-driven**'.[146] Even though these measures have an adverse effect on the rights and values proclaimed in the EU Charter, they have proved to be of little help for law enforcement authorities and intelligence services in the fight against terrorism.[147] Consequently, the EU's counter-terrorism measures, especially the ones that extend to the online environment, are subject to rigorous criticism. The perception of Internet within the scope of debates concerning the fight of terrorism differs greatly from other areas. In this context, the internet is no

[140] See, EDPS, The EDPS as Supervisor of Large-Scale IT Systems and Member of Supervision Coordination Groups, 2015.
[141] Mitsilegas, V., 'Border Security in the European Union: Towards Centralised Controls and Maximum Surveillance' in Baldaccini, Anneliese, Elspeth Guild and Helen Toner (2007), Whose Freedom, Security and Justice? EU Immigration and Asylum Law and Policy, Hart Publishing, Oxford, 2007, 359.
[142] González Fuster, G., de Hert, P., Gutwirth, S., D.2.1. State-of-Art Report on the Current Scholarship on the Law-Security Nexus in Europe, 2008, 22.
[143] Court of Justice of the European Union, Joined Cases *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General* (C-293/12) *and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others* (C-594/12), 8 April 2014.
[144] Court of Justice of the European Union, *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14), 6 October 2015, § 94.
[145] Court of Justice of the European Union, *Breyer v Bundesrepublik Deutschland* (C-582/14), 19 October 2016.
[146] Wensink, W. et al, The European Union's Policies on Counter-Terrorism Relevance, Coherence and Effectiveness, 2017.
[147] Ibid.

longer considered to be the medium facilitating the implementation of human rights, instead it is perceived as a source of '*information on terrorist means and methods*' *such as amount to a 'virtual training camp'*.'[148]

Directive (EU) 2017/541[149] further reaffirms a view point that the internet can *'inspire and mobilise local terrorist networks and individuals'* and it includes the '*public provocation to commit a terrorist offence*' among offences related to terrorist activities (Art. 5) [150] This offence '*has been subject to considerable criticism both because of its wide scope and because of uncertainty about the commitment to fundamental human rights guarantees, notably freedom of expression. The definition of* ***'terrorist offence'*** *is undeniably broad and this breadth is expanded further by the definition of provocation which does not require that the speech actually results in a terrorist act, only that* ***the speech 'causes a danger'*** *that an offence may be committed*.'[151] In this area '*the focus of the EU has been very much on* ***holding individual users liable*** *rather than on imposing liability on service or host providers. This is partly a consequence of worries about allowing governments to censor the Internet and partly due to the practical and financial burdens that would accompany demands that providers monitor all content before it is posted*.'[152] For more information on issues concerning the area of freedom, security and justice, consult Annex III.

4.2 Embedding Value-driven Cybersecurity in Legislation and Beyond

Adhering to the EU Charter requires embedding its values into the applicable regulatory framework. But putting this to practice is not a straightforward task when it comes to development and implementation of EU legislation or policies. The embedment process entails a comprehensive understanding of '*the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities*'[153] as well as a thorough understanding of the regulatory field, such as cybersecurity. The possession of expertise in both areas by one individual and even one organisation is rare and consequently, the embedment process requires a proactive involvement, action and collaboration of different stakeholders. The embedment of EU values enshrined in the EU Charter can take place both on an *ex ante* and an *ex post* basis. [154]

The EU institutions that are exercising a legislative power, namely the European Commission, the Council of EU and the European Parliament, as well as EU agencies can play an important role in this regard on an *ex ante basis*. [155] For example, the European Commission (and to some extent the European Parliament) has developed good practices of carrying out compatibility checks and impact assessments of legislative proposals. It is believed that a combination of a fundamental rights compatibility check and the inclusion of fundamental rights in impact assessments, allows the Commission to mitigate the risk that its proposed measures violate fundamental rights.[156] The knowledge generated during this process then can '*guide the decision-making process to ensure that the course of action that will best support the fulfilment of fundamental rights will be chosen'*. [157] The importance of these tools is challenged during the legislative process, in particular, by amendments that entail considerable changes to a proposed

[148] Summers et al., *The Emergence of EU Criminal Law*, 168.
[149] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA [2017] OJ L88/6.
[150] Summers et al., *The Emergence of EU Criminal Law*, 168.
[151] Summers et al., *The Emergence of EU Criminal Law*, 172.
[152] Ibid., 175.
[153] Ibid., Article 2.
[154] For example, the European Parliament challenged the draft agreement between the European Union and Canada on the transfer of Passenger Name Record at the European Court of Justice; Maximillian Schrems successfully challenged the Safe Harbor Agreement, which governed data transfers between the EU and the USA.
[155] De Schutter, O., The Implementation of the Charter of Fundamental Rights in the EU institutional framework, Study for the AFCO Committee, 2016.
[156] Ibid., 21.
[157] Ibid., 21.

text and relate to the protection of fundamental rights.[158] In the domain of cybersecurity, opinions and contributions of the specialised EU bodies, such as EDPS, ENISA and the Article 29 Working Party, proved to be useful and allowed overcoming the limitations of initial compatibility checks and impact assessments.

The participatory dimension can also facilitate the integration of EU values into regulatory frameworks and policies. For example, during the drafting stage of legislative proposals, the European Commission usually launches a public consultation process in order to unveil the key issues faced by the concerned stakeholders. In fact, the European Commission carries a duty to conduct '*broad consultations with parties concerned in order to ensure that the Union's actions are coherent and transparent*'.[159] Based on the **inputs** received during the **public consultation process**, the European Commission has to propose measures that would not only balance different interests of stakeholders but that also would be compatible with values enshrined in the EU Charter. The concerned stakeholders remain active after these consultations are closed and they provide **comments on legislative proposals** throughout **different stages of legislative process**. Some organisations, in particular, the ones representing civil society groups, often provide detailed analyses of how a future legislative measure could better implement provisions of the EU Charter.[160] However, for these analyses to be taken into account by legislators, the concerned stakeholders need to run lobbying campaigns.

Apart from compatibility checks, impact assessments of legislative proposals and stakeholders' participation, legislators can choose **emphasising certain values** in the **legislative text**. For example, the GDPR introduced the principle of **data protection by design** (DPbD) in Article 25.1. This principle explicitly requires controllers of personal data processing activities to implement technical and organisational measures that would be appropriate to the level of risks that may arise from the processing activities for rights and freedoms of individuals' whose data are being processed.[161] These measures should ensure that the requirements and principles of the GDPR are embedded in the processing activity from its inception as well revised and updated throughout the data processing activity. This principle represents an interesting legislative technique as it in practice reinforces the obligations that are listed in Article 5 of the GDPR specifying the principles of personal data processing (previously found in Article 6 of the Data Protection Directive).

Finally, it seems that even though EU institutional set up allows challenging measures that are not compatible with EU values,[162] more could be done in order to embody EU values in legislative frameworks and policies. It is believed that '***a permanent**, rather than a one-time, **assessment of fundamental rights compatibility of EU legislation***' as well as '*the establishment of **a mechanism** to systematically **screen developments in the Union** in order to identify the need to take action at EU level in order to protect and fulfill the rights, freedoms and principles of the Charter*' would enhance compliance with values embedded in the EU Charter. [163]

[158] Ibid., 21.
[159] Consolidated Version of the Treaty on European Union and the Treaty on the Functioning of the European Union (2010/C 83/01); The Treaty on European Union (TEU), Article 11 (3).
[160] For example, see: EDRi, Proposal for amendments, 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) 2017/0003 (COD), available at: https://edri.org/files/epd-revision/AMS_for_ePREDRi-FINAL.pdf.
[161] GDPR, Article 25.1.
[162] For example, the European Parliament challenged the draft agreement between the European Union and Canada on the transfer of Passenger Name Record at the European Court of Justice; Maximillian Schrems successfully challenged the Safe Harbor Agreement, which governed data transfers between the EU and the USA.
[163] De Schutter, O., The Implementation of the Charter of Fundamental Rights in the EU institutional framework, Study for the AFCO Committee, 2016, 13.

5. Concluding Remarks

This White Paper explored the notions of 'value-driven' and 'cybersecurity' from the perspective of EU law. In relation to values, it has highlighted the significance of those listed in the Treaty of EU, namely '*respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights'*.[164] These values need to be considered within both internal and external EU policies, and may legitimise the expansion of EU competencies and consequently, the adoption of new regulatory measures.[165] Nevertheless, their interpretation, respect and promotion by EU institutions and Member States is not always uncontested.

The main challenges of cybersecurity regulation include the ambiguous use of the term 'cybersecurity', cooperation of stakeholders and securitisation of EU values and interests. The ambiguous use of the term 'cybersecurity' leads to open ended understanding of the regulatory area, which may provide EU legislature with flexibility about issues that can be placed under this 'umbrella' term. At the same time, measures adopted in the name of (cyber)security may fall outside the EU competence.

In order to attain objectives set by 2013 EU Cybersecurity Strategy, cooperation between different stakeholders is crucial. For cooperation to be successful different actors should not only be assigned clear roles and responsibilities but they should also be accountable and transparent about their practices and areas of expertise. The coordination of cooperation remains challenging as it includes numerous public and private stakeholders at EU and national level spread across the following domains 1) network and information security, 2) electronic communications, and 3) criminal justice. Lastly, with the surge of technology use in a wide range of areas, legitimate concerns are raised about information security. As the European Commission has pointed out, there are different scenarios which would allow Member States to pool their industrial and technical resources. While currently cybersecurity issues are addressed via Security and Defence Cooperation, careful reading of its policy documents implies that the EC has a preference for the Common Defence and Security. The choice of the latter would entail a change in EU competence, which may require citizens' approval in some countries.

The White Paper discusses ten controversies over EU value-driven cybersecurity regulation, even though more controversies, reflecting self-defeating strategies, could be established. First, numerous EU policy measures that address cybersecurity issues also recognise that any measures taken with respect to the protection of security of information infrastructures have to be developed '*in accordance with the commitment of the European Union to respect fundamental human rights*'.[166] Nevertheless, there are cases where EU policy measures and legislation do not adhere to principles established in EU fundamental rights. Hopefully, with the enforcement of the Lisbon Treaty and the recognition of the Charter of Fundamental Rights these situations are avoided or reduced to minimum. Second, in order to address and mitigate information security risks, EU regulatory measures rely on proactive individuals and companies who are able to identify risks and act upon them, even though information risks are difficult to quantify, constantly changing and require a certain level of expertise. The current approach of relying on individuals and companies may not be the most effective way to tackle information risks. Third, attribution of roles to different stakeholders is desirable but in some situations, clearly defined roles of actors may reduce the scope of law. Fourth, individuals are being awarded with more rights despite they often lack digital literacy over their existing rights and their enforcement mechanisms. Fifth, the notions of data controllership and ownership have recently resurfaced in discussions about

[164] Consolidated Version of the Treaty on European Union and the Treaty on the Functioning of the European Union (2010/C 83/01); The Treaty on European Union (TEU), Article 2.
[165] European Commission, Reflection Paper on the Future of European Defence, June 2017.
[166] European Commission, Communication, 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime', COM(2000) 890; see also: European Commission, Communication, The Digital Agenda for Europe - Driving European growth digitally, COM(2012) 784 final; Council of the EU, The Stockholm Program: An open and secure Europe serving the citizen, 17024/09.

data policies, in particular at European level. While arguably data controllership or ownership may ensure the better quality of information, in practice, it is a formidable task due to data fluidity. Sixth, enforcement of intellectual property rights (IPRs), in particular, a copy right protection, remains highly contested. Seventh, as notions of 'criminal', lawful', 'harmful' and 'illegal' content are often locked to the political and cultural context, there is little agreement among the Member States about online content regulation. Eighth, even though there is an emerging agreement that installing backdoors to devices or encryption schemas in order to identify criminals and terrorists would reduce security among academics and EU agencies, issues related to encryption are subjected to heated discussions at the EU institutions. Ninth, even though the EU has set up several large-scale IT systems that facilitate surveillance of individuals, it has a clear vision over which massive and generalised surveillance can be acceptable in the EU. Finally, the EU recently penalised terrorist offences in Directive (EU) 2017/541, which has received criticism both because of its wide scope and because of uncertainty about the commitment to fundamental human rights guarantees, notably freedom of expression.

The discussion over controversies demonstrated that values stemming from the EU Charter play an important role in the EU regulatory approach in the cybersecurity domain, even though they are contested by EU institutions, Member States and interests of stakeholders. The White Paper pointed out that a strong emphasis put on the protection and promotion of fundamental rights form a unique and distinctive EU approach to cybersecurity. However, for protection of fundamental rights to become an established principle in the cybersecurity domain, the EU has to consistently advocate for it in its internal and external measures. It seems that even though EU institutional set up allows attaining this consistency by allowing various actors to challenge measures that are not compatible with EU values throughout different stages of development and implementation of legislation and policies.

While a permanent assessment of fundamental rights compatibility of EU legislation as well as the systematic screening of developments concerning the protection of the rights, freedoms and principles of the EU Charter would enhance compliance with values embedded in the EU Charter, there are more ways to embed EU values in legislative frameworks and policies. Perhaps, the most interesting proposal in this regard entails developing new legislative techniques, such as demonstrated by the data protection by design principle, which further strengthens obligations stemming from the GDPR. Indeed, a more accentuated use of existing measures and principles, stemming from EU values, for example, the implementation of appropriate security measures, as required by the EU data protection framework, may benefit the overall cybersecurity.

References

Alheit, K., 'The applicability of the EU Product Liability Directive to Software', Comparative and International Law Journal of Southern Africa, Volume 34, Issue 2, Jul 2001.

Article 29 Working Party, Guidelines on the right to data portability, April 2017.

Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", February 2010.

Benedek, W., Kettemann, M.C., Freedom of expression and the Internet, Council of Europe, 15 Jan 2014.

Black, J., 'The role of risk in regulatory processes' in R. Baldwin, M. Lodge and M. Cave, *Oxford Handbook of Regulation*, Oxford University Press, 2010.

Bryman, A., *Social Research Methods*, Oxford University Press, 2008.

Cf. Note 14711/16 from the Council of the European Union Presidency to the Permanent Representatives Commit-tee/Council on the subject title 'Encryption: Challenges for criminal justice in relation to the use of encryption - future steps - progress report', Brussels, 23 November 2016.

Consolidated Version of the Treaty on European Union and the Treaty on the Functioning of the European Union (2010/C 83/01).

Council of the EU, Presidency Progress report: Encryption: Challenges for criminal justice in relation to the use of encryption - future steps, LIMITE CYBER 137, JAI 976, 14711/16, Brussels, 23 November 2016.

Council of the EU, The Stockholm Program: An open and secure Europe serving the citizen, 17024/09.

Craig, P., *The Lisbon Treaty: law, politics, and Treaty reform*, Oxford University Press, 2013.

Daley, J., 'Insecure software is eating the world: Promoting cybersecurity in an age of ubiquitous software-embedded systems', 19 The Stanford Technology Law Review 533 (2016).

Darmois, E. and Schméder, G., Cybersecurity: a case for a European approach, Paper commissioned by the Human Security Study Group SiT/WP/11/16, 2016.

De Hert, P., Jasmontaite, L., Internet Content Suppression, in De Gruyter et al. *Culture and Human Rights: The Wroclaw Commentaries*, 2016.

De Schutter, O., The Implementation of the Charter of Fundamental Rights in the EU institutional framework, Study for the AFCO Committee, 2016.

Digital Economy and Society Index, Results of the study are available at: https://ec.europa.eu/digital-single-market/en/desi.

Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union.

EDPS, Guidance on Security Measures for Personal Data Processing Article 22 of Regulation 45/2001.

EDPS, Opinion 6/2017 on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation).

EDPS, Opinion 8/2015 Dissemination and use of intrusive surveillance technologies.

EDPS, The EDPS as Supervisor of Large-Scale IT Systems and Member of Supervision Coordination Groups, 2015.

ENISA, Definition of Cybersecurity: Gaps and overlaps in standardization, December 2015.

ENISA, Principles and opportunities for a renewed EU cyber security strategy, ENISA contribution to the Strategy review, May 2017.

Eriksson, J., Giacomello, G., 'The information Revolution, Security and international Relations; (IR)relevant theory?' International Political Science Review, Vol. 27, No. 3, 2006.

European Commission and High Representative of the EU for Foreign Affairs and Security Policy (2013), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013 JOIN(2013) 1 final.

European Commission, Commission Staff Working document 'Comprehensive Assessment of EU Security Policy accompanying the document Communication to the European Parliament, the European Council and the Council: Ninth progress report towards an effective and genuine Security Union' (Part 1), Brussels, 26.7.2017 SWD(2017) 278 final.

European Commission, Commission Staff Working Document, Better Regulation Guidelines, Strasbourg, 19.5.2015 SWD(2015) 111 final.

European Commission, Communication - A strategy for a Secure Information Society - 'Dialogue, partnership and empowerment' {SEC(2006) 656} /* COM/2006/0251 final.

European Commission, Communication 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime', COM(2000) 890.

European Commission, Communication on Seventh progress report towards an effective and genuine Security Union, 16.5.2017 COM(2017) 261 final.

European Commission, Communication to the European Parliament, the European Council and the Council, Seventh progress report towards an effective and genuine Security Union COM(2017) 261 final.

European Commission, Communication, 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime', COM(2000) 890.

European Commission, Communication, eEurope Benchmarking Report - eEurope 2002 /* COM/2002/0062 final.

European Commission, Communication, The Digital Agenda for Europe - Driving European growth digitally, COM(2012) 784 final.

European Commission, Legal study on ownership and access to data, 2016, 978-92-79-62181-9.

European Commission, Reflection Paper on the Future of European Defence, June 2017.

European Commission, Study on Product liability in the European Union, February 2003, Contract No. ETD/2001/B5-3001/D/76.

European Communication, Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All, Brussels, 10.5.2017 COM(2017) 228 final.

European Criminal Policy Initiative, 'Manifesto II'.

European Parliament, Report on the fight against cybercrime, 2017/2068, A motion for a European Parliament Resolution.

European Union Agency for Network and Information Security, 'ENISA's Opinion Paper on Encryption - Strong Encryption Safeguards our Digital Identity', December 2016.

European Union Agency for Network and Information Security, ENISA's Opinion Paper on Encryption Strong Encryption Safeguards our Digital Identity, December 2016.

German CCC publication: 'Chaos Computer Club analyzes government malware', published October 8th 2011.

Gordon, L. A., Loeb M.P., Zhou L., Investing in Cybersecurity: Insights from the Gordon-Loeb Model, Journal of Information Security Vol.7 No.2, 2016.

Hildebrandt, M., Tielemans, L., 'Data protection by design and technology neutral law' Computer law & Security Review 29 (2013) 509-521.

Irish National Cyber Security Centre within the Department of Communications, Energy and Natural Resources, National Cyber Security Strategy 2015-2017.

ITU, Recommendation, ITU-T X.1205.

Kuner, C., 'Data Nationalism and Its Discontents', 2014, 64 Emory Law Journal 2089-2098.

Kuner, C., 'The Internet and the Global Reach of EU Law' (February 1, 2017). Forthcoming, Collected Courses of the Academy of European Law (Oxford University Press); LSE Legal Studies Working Paper No. 4/2017; University of Cam-bridge Faculty of Law Research Paper No. 24/2017. Available at: http://dx.doi.org/10.2139/ssrn.2890930.

Nagurney, A. & Nagurney, L.S., Netnomics, A game theory model of cybersecurity investments with information asymmetry (2015) 16: 127. doi:10.1007/s11066-015-9094-7.

Opinion No. 28 of the European Group on Ethics in Science and New Technologies, 'Ethics of Security and Surveillance Technologies', Brussels, 20 May 2014.

Outcome of the 3508th Council meeting, document 15391/16 and press release 67 by the Justice and Home Affairs department, section 'Criminal justice in Cyberspace', Brussels, 8th and 9th December 2016.

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 L119/1, 4.5.2016.

Regulation (EU) No 526/2013 concerning the European Union Agency for Network and Information Security (ENISA) repealing Regulation (EC) No 460/2004.

Schuman Declaration, 9 May 1950, available at: https://europa.eu/european-union/about-eu/symbols/europe-day/schuman-declaration_en.

Special Eurobarometer 390, Cyber security, Wave EB77.2 – TNS Opinion & Social, 2012.

Speech by Vice-President Ansip at the Chatham House annual cyber conference: Evolving norms, improving harmonisation and building resilience, 26 June, 2017.

Steiner, J., Woods, L. *EU Law*, Oxford University Press, 2012.

Summers et al., *The Emergence of EU Criminal Law*, Hart Publishing, 2014.

Treaty Constituting the European Coal and Steel Community, available at: http://www.consilium.europa.eu/uedocs/cmsUpload/Treaty%20constituting%20the%20European%20Coal%20and%20Steel%20Community.pdf.

Van der Meulen Nicole, Eun A. Jo and Stefan Soesanto (RAND Europe), Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses (2015), available at: http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)536470.

Wensink, W. et al, The European Union's Policies on Counter-Terrorism Relevance, Coherence and Effectiveness, 2017.

Wiewiórowski Wojciech, Privacy, security and technology: the Annual Privacy Forum 2017, available at: https://edps.europa.eu/press-publications/press-news/blog/privacy-security-and-technology-annual-privacy-forum-2017_en.

Jurisprudence

Court of Justice of the European Union, Aklagaren v Hans Akerberg Fransson (C-617/10) 23 February 2013.

Court of Justice of the European Union, Breyer v Bundesrepublik Deutschland (C-582/14),19 October 2016.

Court of Justice of the European Union, Joined Cases Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General (C-293/12) and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others (C-594/12), 8 April 2014.

Court of Justice of the European Union, Maximillian Schrems v Data Protection Commissioner (Case C-362/14), 6 October 2015.

Court of Justice of the European Union, Opinion 1/15 Draft agreement between Canada and the European Union — Transfer of Passenger Name Record data from the European Union to Canada, 26 July 2017.

Court of Justice of the European Union, SABAM v Netlog NV (C-360/10), 16 February 2012.

Court of Justice of the European Union, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (C-70/10), 24 November 2011.

Annex 1: Review of EU Soft-law Measures Addressing Cybersecurity*

With more information vanishing into cyberspace, the use of term 'cybersecurity' has dramatically increased. Policy makers, regulators, activists, business representatives, journalists and ordinary citizens – all have an opinion on how best to address this issue. We have prepared this annex with an aim to contribute to the ongoing discussion with regard to cybersecurity. In particular, we will try to explain how the term 'cybersecurity' has emerged in the EU. To this end, in this annex we will analyse numerous EU policy documents that have shaped this term. A better understanding of contexts and agendas in which this term has originated, can lead us to a greater understanding of the EU cybersecurity policy and its underlying objectives.

The review presents EU policy documents, such as communications, Council resolutions and implementation reports that address issues of information systems and networks security. The reviewed documents cover the period of 2000-2016. The selected documents are presented in chronological order as this particular structure of the review allows tracking down the development of EU cybersecurity policy, including the emergence of the term 'cybersecurity'. In order to find the first documents addressing issues related to cybersecurity, the authors relied on references included in policy documents to earlier documents, which are followed up, related or addressed similar issues. All of the reviewed documents are available in EU bibliographical databases and can be accessed on the Internet.

The presidency conclusions of the Lisbon European Council (often referred to as the Lisbon Strategy) is one of the first high-level policy documents that paved the way for regulatory developments concerning the online environment. The Lisbon Strategy (Strategy) included a roadmap of key EU objectives. According to this roadmap, the EU had 'to become the most competitive and dynamic knowledge-based economy in the world' by 2010.[167] Among other objectives, the Lisbon Strategy aimed at ensuring that the EU information society can adapt to a knowledge-based digital economy, which was considered to be 'a powerful engine for growth, competitiveness and jobs'.[168] The Strategy observed that the EU has to find a way to modernise its social protection model in the context of emerging digital reality. In particular, the Strategy foresaw the need 'to strengthen cooperation between Member States by exchanging experiences and best practice on the basis of improved information networks which are the basic tools in this field'.[169] While the Strategy focused on setting policies and appropriate legal frameworks for attaining 'e-potential' by accessible information technologies and advancement of digital skills, it invited the Council of the EU (Council) and the European Commission (Commission or EC) to develop a comprehensive eEurope Action Plan.

The EC Communication **'eEurope 2002: Impact and Priorities'** was an integral part of the Lisbon Strategy and further specified measures to be adopted and developed with a view to achieving the following three main objectives: 1) cheaper, faster and more secure Internet access, 2) increased investment in citizens' digital skills, 3) and incentives for the use of the Internet.[170] To enhance user confidence in the field of electronic commerce, the Action Plan proposed the following measures:

* This section has been written by Lina Jasmontaite (Vrije Universiteit Brussel).

[167] European Council, Presidency conclusion of the Lisbon European Council of 23 and 24 March 2000 (Lisbon Strategy), available at: http://www.europarl.europa.eu/summits/lis1_en.htm, 5.

[168] Ibid., 8.

[169] Ibid., 31.

[170] European Commission, Communication 'eEurope 2002: Impact and Priorities', 23-24 March 2001 COM/2001/0140 final, 5-9.

1. support industry-led security certifications through coordination of efforts and mutual recognition;
2. promote privacy-enhancing technologies, including proper codes and the consolidation of practice;
3. stimulate public/private cooperation on dependability of information infrastructures.

In the **eEurope Benchmarking Report - eEurope 2002**, it was pointed out that 'for computers and communication networks everywhere, security has become a major concern. During the short period of eEurope, there has been a visible increase in threats and security incidents. Virus attacks in particular have become much more common' whereas progress to improve protection against security threats was considered to be slow.[171]

In this regard, the **Communication** titled **'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime'** can be seen as the first elaborate policy document focusing on cybersecurity issues. This communication recognized that '[i]nformation and communication infrastructures have become a critical part of [EU economy]'and called for 'a comprehensive policy initiative' that would allow enhancing the security of information infrastructures and combat cyber-crime.[172]

This Communication posited that individuals play a crucial role with regard to information security. The Communication pointed out that 'to an important extent [is] a responsibility of the users, as only they can appreciate the value of the bits being sent or received, and can determine the level of protection needed'. [173] The Communication, building on the observation of individuals' deep involvement online, went further and suggested that '[t]he user environment is therefore a key part of the information infrastructure. Security techniques have to be implemented there with the permission and participation of the user and according to his/her needs.'[174]

The Communication facilitated the establishment of an EU Forum on cybersecurity and cybercrime, yet it recognized that these different initiatives are not sufficient to provide for higher network security. Therefore, the Commission called for a more comprehensive framework, which at the time, due to the three-pillar structure of the EU, was rather provocative. Interestingly, the Communication has noted that any measures taken with respect to the protection of security of information infrastructures have to be developed 'in accordance with the commitment of the European Union to respect fundamental human rights'.[175]

The **Communication** titled **'Network and Information Security: Proposal for A European Policy Approach'** was developed in a response to the request of the Stockholm European Council in 2001. The starting point of this Communication was the observation that 'finding an adequate policy response is becoming an increasingly complex task'.[176] This communication did not employ the term 'cybersecurity'; rather, it focused on network and information security which, at that time, was 'understood as the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions'.[177] It can be suggested that when reflecting on security threats, the Communication lacked evidence supporting its claims about any potential threats. For example, instead of elaborating on a particular type of threat or context in which security threat could occur, the Communication included bold sentences like this:

[171] European Commission, Communication 'eEurope Benchmarking Report - eEurope 2002', COM/2002/0062 final, 15.
[172] European Commission, Communication 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime', COM(2000) 890, 2.
[173] Ibid., 9.
[174] Ibid., 10.
[175] Ibid., 2.
[176] European Commission, Communication 'Network and Information Security: Proposal for A European Policy Approach', COM(2001) 0298, 2.
[177] Ibid., 3.

'Companies relying on the network for sales or to organise delivery of supplies can be paralysed by a denial of service attack. Personal and financial information can be intercepted and abused. National security can be threatened.'[178]

Nevertheless, the Communication is worth consideration as it proposed the list of measures to tackle security challenges:[179]

- Awareness raising;
- A European warning and information system (e.g., development of Computer Emergency Response Teams (CERTs) and their co-ordination);
- Technology support (e.g., support for research and development in EU funding schemes);
- Support for market oriented standardisation and certification;
- Legal framework;
- Security in eGovernment (i.e., effective and interoperable security solutions in their e-government and e-procurement activities); and
- International co-operation.

The Council issued several resolutions as a follow up of the EC communications and other initiatives. The Council Resolution **'eEurope Action Plan: Information and Network Security'** elaborated further on EU goals with regards to information security and the digital environment. It stated that the Council together with the Commission should lay the ground for measures ensuring security (trustworthiness) of the digital environment. Indeed, it is reasonable to believe that information and network security is the 'prerequisite for the widespread use of information and communication technologies'.[180]

The **Council Resolution on a common approach and specific actions in the area of network and information security** was published in early 2002. The Resolution stressed that information communication systems are not only of a significant economic and social importance but also their availability is at the essence of essential infrastructures.[181] With this observation in mind, the Resolution argued that the protection of information systems is of a growing public interest and therefore, policy with specific measures has to developed to this end. These measures should be holistic and take into consideration the nature and complexity of network and information security as well as political, economic, organisational and technical aspects. The Resolution emphasised the need for more research activities on 'security mechanisms and their interoperability, network reliability and protection, advanced cryptography, privacy enhancement technologies and security in wireless communications'. [182] The Resolution explicitly referred to the international standards, namely ISO-15408 on Evaluation criteria for IT security and ISO-17799 on Information technology - Code of practice for information security management. Furthermore, with this Resolution the Council insisted that Member States take measures to promote adoption of these internationally recognised standards. The Resolution invited 'private sector suppliers and service providers and their representative groupings to participate more actively in international standardisation activities'. [183] It requested that both suppliers and service providers regard security 'as an integral and essential part of their products and services'.[184] Furthermore, the Resolution invited (i.e., asked) Member States to develop awareness raising and education campaigns for business, individual users and public administrations. In particular, the Resolution asked the Member States to consider the effectiveness of national cybersecurity capabilities, such as 'ability to prevent, detect, and react efficiently at

[178] Ibid., 9.
[179] Ibid., 4.
[180] Council of the European Union, Council resolution, e-Europe Action Plan: Information and Network Security, Brussels, 11 June 2001, 9799/01, LIMITE, 2.
[181] Council of the European Union, Council resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security (2002/C 43/02), 43/3.
[182] Idem.
[183] Ibid., 43/4.
[184] Ibid., 43/3.

national and international level against network and information systems disruption and attack'.[185]

In 2003 followed the **Council Resolution on a European approach towards a culture of network and information security**. While the document was rather short, it allowed to further clarify the EU role within the domain of information security, often referred to as cybersecurity.

The Resolution noted that a secure digital environment is instrumental for citizens, businesses and public administrations as well as for the proper functioning of the Internal Market.[186] The reference to the Internal Market is of great significance. As it will be demonstrated later, subsequently, it enabled further EU action and harmonization of Member States approaches in the cybersecurity context.

While calling for a culture of network and information security, the Resolution invited both Member States and the EU institutions to work on a strategy for network and information security that would take into consideration international cooperation and good practices, such as the OECD Guidelines for the security of Information Systems and Networks. The Resolution echoed ideas of previous policy documents and noted that 'a coherent security policy development at European level requires cross-pillar transparency and cooperation'.[187] The Resolution, while recognizing that confidence (trustworthiness) of networks and information systems is of great importance for citizens and enterprises, encouraged employing a holistic view specifying responsibilities of all stakeholders. It invited all actors to take adequate measures to respond and prevent security incidents. The Resolution welcomed actions initiated by the European Commission, namely, [188]

- the application of the open method of coordination
- the set up a temporary interdisciplinary working group
- the establishment of a Cyber-Security Task Force
- building a dialogue with industry to improve security in the development of hardware and software products and ensure the availability of services and data;
- the establishment contacts with relevant international partners and international organizations.

Last but not least, the Resolution emphasized that regulatory and policy actions should take into consideration and respect 1) democratic values, 2) the importance of personal data protection, and 3) privacy rights.[189]

In 2005 the Commission, published the Communication '**i2010 – A European Information Society for growth and employment**.' This Communication for the first time included more precise estimations of the ICT impact on the European society. In particular, the Communication claimed that 'a quarter of EU GDP growth and 40% of productivity growth are due to ICT'.[190] The Communication also recognized that '[i]nformation and communication technologies are a powerful driver of growth and employment'.[191] The Communication outlined an action plan to meet the following three objectives:

- Objective 1: A Single European Information Space offering affordable and secure high bandwidth communications, rich and diverse content and digital services.
- Objective 2: World class performance in research and innovation in ICT by closing the gap with Europe's leading competitors.

[185] Ibid., 43/4.
[186] Council of the European Union, Council resolution, of 18 February 2003 on a European approach towards a culture of network and information security, 48/1.
[187] Idem.
[188] Ibid., 48/2.
[189] Ibid., 48/1.
[190] European Commission, Communication 'i2010 – A European Information Society for growth and employment', COM(2005) 229 final, 3.
[191] Idem.

- Objective 3: An Information Society that is inclusive, provides high quality public services and promotes quality of life.

This Communication introduced terms that still dominate debates on cybersecurity regulation, namely: 'trustworthy, secure and reliable'. It can be suggested that by invoking these terms, the Commission recognised that the understanding of ICT is dynamic and changes over time. From the primary focus on security, the attention has shifted to other characteristics and qualities of the ICT, namely trustworthiness and reliability. The Communication foresaw the adoption of a Strategy for a Secure Information Society that would to lead to changes in a legislative framework and awareness campaigns. The Communication also explained in greater detail the EC's commitment to foster research and innovation efforts that would 'design-in' security and facilitate deployment of measures that test solutions for key issues such as identity management.[192] In order to establish 'a consistent internal market framework for information society and media services', the Communication noted that it is necessary to review legislative frameworks applicable to protection of privacy, electronic signature or discouraging illegal and harmful content. [193]

In 2006 the Communication 'Strategy for a Secure Information Society – Dialogue, partnership and empowerment' was published. This Communication not only outlined more specific measures that the EU was going to take but it also placed the debates on the ICT security within a wider context. In particular, the Communication stressed that the EU has an important role to play within the scope of debates taking place at international level, for example, at the OECD, the Council of Europe or the UN. To further advance the discussions at international level, it was necessary to develop a common understanding of the issues of Internet security. Indeed, the EU (as a unit representing 28 countries) may have a stronger impact in international debates considering fight against cybercrime and spam while ensuring the protection of privacy and freedom of expression.

The Communication noted that 'effective policy making needs a clear understanding of the nature and extent of the challenges'.[194] The ambition to understand these challenges is to a large extent reflected in the EU response to security challenges, which has resulted in 'a three-pronged' approach including:

- specific network and information security measures,
- the regulatory framework for electronic communications (which includes privacy and data protection issues), and
- the regulatory framework for the fight against cybercrime.[195]

The Report on the Implementation of the European Security Strategy was published in 2008. While following on the previous actions of the European Security Strategy developed back in 2003, the Report expanded the list of security challenges to the EU. In particular, the Report regarded information systems and energy supply as the vulnerable 'arteries of our society'.[196] The Report noted that 'globalisation is accelerating shifts in power and is exposing differences in values'.[197] The Report concluded that the EU should develop a comprehensive approach tackling cyber security issues. The Report reasoned the EU should go beyond criminalisation of unlawful activities and consider new dimensions of cyber security that relate to economy, policy and military. Additionally, the Report stressed the need for further work with regards to awareness raising and international co-operation.[198]

[192] Ibid., 6.
[193] Ibid., 6.
[194] European Commission, Communication 'A strategy for a Secure Information Society - 'Dialogue, partnership and empowerment', COM/2006/0251 final, 8.
[195] Ibid., 3.
[196] Council of the EU, Report on the Implementation of the European Security Strategy - Providing Security in a Changing World – 2008, 1.
[197] Ibid., 1.
[198] Ibid., 5.

The Stockholm Program: An open and secure Europe serving the citizens can be considered to be a more thorough follow up of the European Security Strategy. The European Council with this document set a framework for the EU action outside the first pillar structure for the period of 2010 – 2014. The Program tackled issues related to citizenship, justice, security, asylum, immigration and visa policy. This Program claimed that '[t]he challenge will be to ensure respect for fundamental freedoms and integrity while guaranteeing security in Europe'.[199] The Program observed that on political level it is necessary to develop mutually reinforcing measures. To this end, the Program suggested that 'law enforcement measures and measures to safeguard individual rights, the rule of law, international protection rules go hand in hand in the same direction'.[200] The Program focused on protecting citizen's rights in the information society and proclaimed that the EU carries a duty to 'respond to the challenge posed by the increasing exchange of personal data and the need to ensure the protection of privacy'.[201] In particular, the Program insisted that the EU develops 'a comprehensive strategy to protect data within the EU and in its relations with other countries', while promoting the application of the principles set out in relevant EU instruments on data protection and the 1981 Council of Europe Convention on data protection.[202] Additionally, the Program stressed that the EU has to specify situations in which interference by public authorities with the exercise of these rights is justified. Data protection principles must be also applicable in the private sphere. Furthermore, the Program concluded that '[b]asic principles such as purpose limitation, proportionality, legitimacy of processing, limits on storage time, security and confidentiality as well as respect for the rights of the individual, control by national independent supervisory authorities, and access to effective judicial redress need to be ensured and a comprehensive protection scheme must be established.'[203] Finally, the European Council was of an opinion that 'the Union must address the necessity for increased exchange of personal data whilst ensuring the utmost respect for the protection of privacy'.[204] From the statements provided in the Program it can be suggested that the European Council is a techno-optimist. It considers that technological advancements not only pose challenges to the protection of personal data but also provide for new ways to run business and protect personal data.

Another important aspect of the Program was mobilising the necessary technological tools, as well as the legislative framework ensuring a high level of network and information security protection, including protection of critical infrastructures, Information and Communication Technology (ICT) and services infrastructure. The Program insists that the EU encourages 'policies and legislation that ensure a very high level of network security and allow faster reactions in the event of cyber disruptions or cyber attacks'. These tools and measures should ensure that people are safe, secure and free. In summary, it can be claimed that while the European Council regarded the protection of network information systems and the fight against cyber-crime as two separate elements to the overall security of the EU, in both cases any measures developed in the context of these frameworks should reinforce the exercise of citizens' rights, in particular the rights to privacy and the protection of personal data. The Program called for a coherent policy response which goes beyond the area of freedom, security and justice.

Despite all the effort and measures tackling information security challenges, these measures were considered in isolation and a more coherent approach with regard to information communication systems was necessary. To this end, the Communication published **'A Digital Agenda for Europe'** in 2010. The starting point of this document was the observation that '[p]eople's enjoyment of digital technologies, be it as citizens, consumers or workers, is marked by privacy and security concerns, by insufficient internet access, insufficient usability, by lack of relevant skills or by lack of accessibility for all'.[205] The

[199] Council of the EU, The Stockholm Program: An open and secure Europe serving the citizen, 17024/09 (2009), 3.
[200] Idem.
[201] Ibid., 18.
[202] Idem.
[203] Idem.
[204] Idem.
[205] European Commission, Communication 'A Digital Agenda for Europe', COM/2010/0245 f/2, 5.

Communication was of opinion that 'a lack of trust in the online environment is meanwhile seriously hampering the development of Europe's online economy'.[206] Indeed, people who did not purchase online were reported to have concerns over: payment security, privacy, and trust.

The Communication devoted a section addressing issues related to trust and security. The Communication insisted that [u]sers must be safe and secure when they connect online and therefore criminal activities, motivated by financial or political purposes, including identity theft and online fraud, in the digital space should not be acceptable. Yet addressing these challenges was considered to be a shared responsibility – everyone has a role to play within their respective capacity. One of the reasons to revise the framework for electronic communications was the pressing need to clarify roles and the responsibilities of network operators as well as service providers.

The Communication explicitly noted that '[t]he right to privacy and to the protection of personal data are fundamental rights in the EU which must be – also online - effectively enforced using the widest range of means: from the wide application of the principle of 'Privacy by Design' in the relevant ICT technologies, to dissuasive sanctions wherever necessary.' [207]

The Communication integrated the protection of critical information infrastructure and the agenda for freedom, security and justice, set forth by the Stockholm Program: An open and secure Europe serving the citizen. The Communication used the term cybersecurity only when discussing information security aspects from the international perspective.

Given the fast pace of technological developments, the list of actions was revised in 2012. The Digital Agenda - Driving European growth digitally did not further advance discussions on the issues related to cybersecurity. The Digital Agenda 2012 advocated for the development of measures 'fostering a secure and trustworthy internet environment for users and operators, based on strengthened European and international collaboration in responding to global risks'.[208] In particular, it paved the way for the adoption of the Directive that would strengthen network and information security across the EU and ensure the smooth functioning of the internal market. The Digital Agenda 2012 employed the typical language for trust and security rather than cybersecurity.

It is noteworthy that the term 'cybersecurity' in its more comprehensive sense to the EU discussions (i.e., going beyond cybercrime) was brought in after 2013. It can be suggested that the Digital Agenda for Europe Scoreboard 2012 and the Special Eurobarometer study 'Cyber security' were among the first documents that introduced cybersecurity as a broader term covering various issues related to the digital environment. The Digital Agenda for Europe Scoreboard 2012 observed that '[c]ybersecurity is rising in prominence as a major policy challenge. Cooperation in this field has been strengthened, for example through the European Forum for Member States and the European Public-Private Partnership for Resilience as well as by the establishment of national/governmental CERTs (computer emergency response teams) in 23 Member States.'[209] The Special Eurobarometer study examined EU citizens' experiences and perceptions of cyber security issues.[210] In the context of the survey, cyber security was used as a phrase capturing citizens' behaviour and actions online.

A comprehensive EU Cybersecurity Strategy was published in 2013. Following up on this document, in 2015 the Commission published the Communication on A Digital Single Market Strategy for Europe. This document further strengthened EU claims for competences to regulate the cybersecurity domain in earlier policy documents. In particular, the 2015 Digital Single Market Strategy, which reasoned that because of the potential impact that lack of trustworthiness in services provided online has on the EU

[206] Ibid., 12.
[207] Ibid., 17.
[208] European Commission, Communication 'The Digital Agenda for Europe - Driving European growth digitally', COM(2012) 784 final, 4.
[209] European Commission, Digital Agenda for Europe Scoreboard 2012, 7.
[210] Special Eurobarometer 390, Cyber security, Wave EB77.2 – TNS Opinion & Social, 2012.

economy, '[a] more joined-up approach is therefore needed to step up the supply of more secure solutions by EU industry and to stimulate their take-up by enterprises, public authorities, and citizens'.[211] Providing an effective legal framework with regards to the protection of the EU fundamental rights as a well as law enforcement activities has been recognised as a priority. To this end, the Commission proposed updating the existing legal framework governing the protection of privacy and personal data and setting up a public-private partnership on cybersecurity.

The European Agenda on Security was also published in 2015. Interestingly, the term of cybersecurity in this document differs from the Digital Single Market Strategy for Europe as cybersecurity is considered to be 'the first line of defence against cybercrime'.[212] This document anticipated that the Directive on network and information security will enhance cooperation between different competent authorities addressing cybersecurity issues (i.e., law enforcement and cybersecurity authorities). More specifically this Agenda foreseen the following action points:

- emphasise the implementation of existing policies on cybersecurity, attacks against information systems, and combatting child sexual exploitation;
- consider extending legislation on combatting fraud and counterfeiting of non-cash means of payments to take account of newer forms of crime and counterfeiting in financial instruments; revision of obstacles to criminal investigations on cybercrime, notably on issues of competent jurisdiction and rules on access to evidence and information;
- enhance cyber capacity building action under external assistance instruments.[213]

The Commission Communication on Strengthening Europe's Cyber Resilience System was published in 2016. This Communication followed up on the previous policy documents, namely the EU Cybersecurity Strategy and the Digital Single Market Strategy. The Communication summarises the EU achievements within the domain of cybersecurity so far and outlines further measures increasing EU cyber resilience. The Communication brought the EU debates on cybersecurity further by considering ways to assess the risk and impact of potential large-scale cyber incident which may occur due to interdependence of cross-border and cross-sectoral communication and information systems.[214]

[211] European Commission, Communication 'A Digital Single Market Strategy for Europe', COM(2015) 192 final, 13.
[212] European Commission, Communication 'The European Agenda on Security Strasbourg', COM(2015) 185 final, 19.
[213] Ibid., 20.
[214] European Commission, Communication 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry', COM(2016) 410 final 6-7.

Annex 2: EU Legislative Measures on Cybersecurity

The table below provides an overview of existing EU legislative measures constituting EU cybersecurity framework. After introducing a regulatory measure, the following column considers if it has been revised, amended or repealed. The last column of the table explains how each regulatory measure contributes to the domain of cybersecurity.

No.	Regulatory measure	Updates and revisions	Relation to cybersecurity
1.	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	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	Requires Member States to ensure controllers and processors to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
2.	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)	Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws	Requires Member States to ensure that providers of a publicly available electronic communications service to take appropriate technical and organisational measures to safeguard security of their services, if necessary in conjunction with the provider of the public communications network with respect to network security. The same article requires providers of a publicly available electronic communications service in case of a particular risk of a breach of the security of the network to inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.
3.	Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography	Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA	Foresees measures against websites containing or disseminating child pornography. In particular, this article requires Member States to take the necessary measures to ensure the prompt removal of web pages containing or disseminating child pornography hosted in their territory

No.	Regulatory measure	Updates and revisions	Relation to cybersecurity
			and to endeavour to obtain the removal of such pages hosted outside of their territory. While Member States are allowed to take measures to block access to web pages containing or disseminating child pornography towards the Internet users within their territory, these measures must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction.
4.	Council Framework Decision 2005/222/JHA, OJ L 69, 16/03/2005 on attacks against information systems	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	Requires Member States to take the necessary measures criminalising: - illegal access to information systems - illegal system interference - illegal data interference
5.	Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing	Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (2015)	Requires Member States to prohibit their credit and financial institutions from keeping anonymous accounts or anonymous passbooks; imposes customer due diligence obligations.
6.	Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters	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	Requires Member States to take measures ensuring a high level of protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data in the framework of police and judicial cooperation in criminal matters.
7.	Council Directive 2008/114/EC on the identification and designation	N/A	- Establishes a procedure for the identification and designation of European critical infrastructures ('ECIs'), and a common approach

No.	Regulatory measure	Updates and revisions	Relation to cybersecurity
	of European Critical Infrastructures and the assessment of the need to improve their protection		to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people. - Requires ECIs to have the operator security plan ('OSP') procedure which identifies the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection.
8.	Commission Regulation No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications		Specifies a procedure for the notification of personal data breaches by providers of publicly available electronic communications services.
9.	Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union		- Lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market. - Requires to take technical and organisational measures that are appropriate and proportionate to manage and mitigate the risk posed to the security of network and information systems which they use in their operations. - Introduces auditing requirements for the taken measures. - Introduces a notification obligation of incidents having a significant impact on the continuity of the essential services they provide.

Annex 3: Cybersecurity and Criminal Justice*

This annex provides and overview of cybersecurity challenges and controversies within the EU criminal justice affairs. The fight against cybercrime constitutes an essential part of cybersecurity, although it addresses a limited subset of threats. As cybercrime is endangering our societies from the online world, criminal justice contributes to protect our assets and uphold our values in the cyberspace. Cybercrime is inseparable from criminal law since it is defined by the latter. But it is important to note that fighting against cybercrime is not merely a legal issue. The THOR concept presents four dimensions of the problem: (T)echnical, (H)uman, (O)rganisational, and (R)egulatory, the regulatory dimension being "related to law provisioning, standardisation and forensics".[215]

In this section on cybersecurity and criminal justice, we will begin with a state-of-the-art review of the current legislation and legal mechanisms. Then we will turn to the numerous challenges and controversies. Finally, we will reflect on the EU values at stake and their dynamics.[216] Our discussion will focus on the legislation common to all Member States. The situation is already complex enough at the EU level, so we will not address national disparities here. However, our subject is purposely at the intersection of cybersecurity, criminal justice, and fundamental rights. We cannot therefore isolate the 'justice' dimension from these other two dimensions of 'security' and 'freedom'.[217]

A3.1 State of the Art

First of all, we need to outline the present legal situation regarding cybercrime in the EU. To this aim, we will consider in turn criminal law and its main areas, the rationale and mechanisms for its harmonisation, the legislation in force at the European level, and its implementation by Member States.

What is crime? Its nature is widely debated. What is considered as crime changes from place to place and evolves through time. The only thing that all criminal acts have in common is that they are prohibited by the state.[218] Criminal law determines what conduct constitutes an offence and what corresponding penalty is applicable.

There is no offence nor penalty without law.[219] Criminal conduct must be clearly defined and delimited. As Article 7 of the *European Convention on Human Rights* (ECHR) states: "No one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national or international law at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the criminal offence was committed."[220]

Criminal (or penal) law is a subdomain of the law. There are other legal means of enforcement such as civil or administrative sanctions. But the criminal law response is used as a last resort: only the most serious acts and omissions are criminalised, i.e. made into crimes. What then is the difference between criminal penalties and other types of sanctions?

---

* This section has been written by Florent Wenger (Université de Lausanne) and David-O. Jaquet-Chiffelle (Université de Lausanne).

[215] Choraś and Kozik, *CAMINO Roadmap*, 7.

[216] This threefold plan is motivated by the CANVAS project proposal for this section of this deliverable.

[217] For instance, the police contribute to security efforts, but are also responsible for law enforcement.

[218] 'CYBERROAD D-3.1', 8.

[219] Klip, *European Criminal Law*, 196ff.

[220] *Convention for the protection of human rights and fundamental freedoms* [1950] ETS No.005.

According to the European Court of Human Rights (ECtHR), the legal classification of an offence under national law is not decisive. Following the so-called Engel criteria[221], the ECtHR in Strasbourg has ruled that "the criminal nature of the penalty can be deduced from both the general character of the rule and the purpose of the penalty, which relate to deterrence and to its punitive nature."[222] Therefore, criminal sanctions are established as a punishment and meant to be dissuasive.[223]

Criminal law is generally divided into substantive law and procedural law. The former encompasses the definition of offences and their penalties, while the latter sets the framework for criminal investigation and proceedings. In the fight against cybercrime (or any crime), both substantive and procedural law are important and interdependent.

A3.1.1 Harmonisation

Criminal law was historically a matter of national sovereignty. However, many areas of crime often have a cross-border dimension. Within Europe, "[d]ifferences in the criminal laws of the Member States are often referred to as providing criminals with an advantage, by allowing them to choose the Member State with the most lenient laws or simply by making the prosecution and investigation of crime more complicated."[224] This is especially true in cyberspace: offenders can benefit from legal loopholes and operate from digital havens because all countries are internetworked.

This is why "criminal law, once considered the preserve of the nation state, has increasingly become subject to 'outside' involvement."[225] Regarding cybercrime, significant efforts have been made by the Council of Europe (CoE) and the European Union (EU). CoE and EU mechanisms are different but they share the same goal: combating transnational crime by harmonising national laws and improving international cooperation in criminal matters.

CoE treaties include conventions and their additional protocols. Although all 28 EU Member States are also members of the CoE, this does not imply that every EU Member State has signed and ratified (or later acceded to) any particular CoE instrument. Each treaty has its own chart of signatures and ratifications by member and non-member states, with their respective dates of entry into force. The states party to a CoE treaty commit to implementing its provisions in their national legal systems.

At the EU level, the situation is more complex. The Union's competence has radically changed since 2009 with the Lisbon Treaty. According to treaties, EU institutions have the authority to legislate in limited areas, in which EU law overrides domestic laws. There are several types of EU legal acts, including regulations and directives which are binding for all Member States, although in a different way.[226] Prior to the coming into force of the Treaty of Lisbon, there was another kind of legislative act which was specific to criminal justice: the framework decision. Existing framework decisions continue to be applicable until they are repealed but they are now being converted into directives.[227]

According to Article 83(1) TFEU, the Union may "establish minimum rules concerning the definition of criminal offences and sanctions in areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis. These areas of crime are the following: terrorism, trafficking in human beings and sexual

[221] Cf. ECtHR, *Engel and others v. the Netherlands*, 8 June 1978, Series A no. 22, paras. 80-82.
[222] Klip, *European Criminal Law*, 2.
[223] These and other functions of criminal penalties are debated, but this issue is outside the scope of this paper.
[224] Summers et al., *The Emergence of EU Criminal Law*, 276.
[225] Ibid., 5.
[226] "Regulations apply to all Member States, and automatically become part of the law of each Member State without the State having to incorporate the measure into its domestic law: they are thus 'binding' in their entirety and 'directly applicable'. (…) Directives differ from regulations in that … while they are binding as to the result to be achieved, they leave the Member States scope to determine the form and the method of their implementation in national law." (Ibid., 21–22)
[227] Ibid., 46.

exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime [i.e. cybercrime] and organised crime."

These ten offences are the so-called 'Euro crimes'.[228] "Of the ten offences that are mentioned … only for 'illicit arms trafficking' has no criminal legislation been adopted [so far]."[229]

Article 83(2) TFEU also allows the EU to "establish minimum rules with regard to the definition of criminal offences and sanctions if the approximation of criminal laws and regulations of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to a harmonisation measure".[230] Moreover, Article 325(4) TFEU enables EU institutions to "adopt the necessary measures in the fields of the prevention of and fight against fraud affecting the financial interests of the Union". Together, these provisions define the scope for EU criminal law.

A3.1.2 Legislation

"Cybercrime law is a continuously evolving process."[231] Moreover, "European criminal law deals with a multi-layered patchwork of legislation and case law."[232] There is no such thing as an EU criminal code: the relevant dispositions are scattered across a series of legal acts. But what is (and what is not) cybercrime? "Despite the extensive legal framework on cybercrime, neither law nor academic research provide for a common definition or classification of cybercrime. The great variety of offences that are usually referred to as cybercrimes makes it difficult to define uniform criteria for differentiating cybercrimes from other criminal offences. Similarly, there is no commonly accepted classification or categorisation of cybercrime."[233] Here below is an inclusive overview of the current cybercrime legislation. For more details, the reader is referred to the E-CRIME[234], EVIDENCE[235] and FIDUCIA[236] projects reports.

As for CoE treaties, there are the Budapest *Convention on Cybercrime* and its *Protocol on Xenophobia and Racism*[237], the Lanzarote *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*[238], the *Convention on Mutual Assistance in Criminal Matters*[239] and the *Convention for the Protection of Human Rights and Fundamental Freedoms*[240] (with their additional protocols).

Chronologically at the EU level[241], the relevant acts enacted before the Lisbon Treaty reform (but still in force to date) include *Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society*[242], *Framework Decision 2001/413/JHA combating fraud and*

---

[228] Cf. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Towards an EU Criminal Policy: Ensuring the effective implementation of EU policies through criminal law*, Brussels 20.9.2011, COM/2011/0573 final.
[229] Klip, *European Criminal Law*, 231.
[230] These areas are: spam; intellectual property; unauthorised entry, transit and residence (illegal immigration); employment of illegal migrants; environmental crime, including ship-source pollution; racism and xenophobia; insider dealing and market manipulation. (Summers et al., *The Emergence of EU Criminal Law*, 70–76)
[231] Koops and Robinson, 'Digital Evidence and Computer Crime', 182.
[232] Klip, *European Criminal Law*, 1.
[233] 'FIDUCIA D-9.2', 93.
[234] 'E-CRIME D-3.2', 21–48.
[235] 'EVIDENCE D-3.1', 15–39.
[236] 'FIDUCIA D-9.3', 5–32.
[237] *Convention on cybercrime* [2001] ETS No.185. *Additional protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* [2003] ETS No.189.
[238] *Convention on the protection of children against sexual exploitation and sexual abuse* [2007] CETS No.201.
[239] *European convention on mutual assistance in criminal matters* [1959] ETS No.030.
[240] *Convention for the protection of human rights and fundamental freedoms* [1950] ETS No.005 (better known as the *European convention on human rights*).
[241] We do not distinguish between substantive and procedural law because legal acts affect either one or both.
[242] *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society* [2001] OJ L167/10.

counterfeiting of non-cash means of payment[243], *Framework Decision 2002/465/JHA on joint investigation teams*[244], *Framework Decision 2002/584/JHA on the European arrest warrant and the surrender procedures between Member States*[245], *Directive 2002/58/EC on privacy and electronic communications*[246] and *Directive 2009/24/EC on the legal protection of computer programs*[247].

The cybercrime-related acts passed under the Treaty of Lisbon are *Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography*[248], *Directive 2013/40/EU on attacks against information systems*[249], *Directive 2014/41/EU regarding the European investigation order in criminal matters*[250], the *General Data Protection Regulation (EU) 2016/679*[251], *Directive (EU) 2016/680 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*[252] and finally *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*[253].

A3.1.3 Implementation

All the above-mentioned EU legal acts are binding for (nearly[254]) all EU Member States. "However, like a Directive, a Regulation cannot of itself and independently of implementing national law, determine or aggravate criminal responsibility. (…) The same goes for obligations that result from a Framework Decision."[255] Indeed, "the principle of legality … requires that criminal liability finds its basis in national criminal law. Direct applicability of Union law, without national transposition, is prohibited."[256]

Implementation by each state in its particular legal system is therefore necessary. As for EU directives, all Member States must take transposition measures and communicate them to the Commission. The latter issues reports assessing the implementation progress and comparing the resulting legislations

[243] *Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment* (2001/413/JHA) [2001] OJ L149/1.
[244] *Council Framework Decision of 13 June 2002 on joint investigation teams* (2002/465/JHA) [2002] OJ L162/1.
[245] *Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States* (2002/584/JHA) [2002] OJ L190/1.
[246] *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)* [2002] OJ L201/37.
[247] *Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs* [2009] OJ L111/16.
[248] *Directive 2011/93/EU* (initially published with duplicate number 2011/92/EU) *of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA* [2011] OJ L335/1.
[249] *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* [2013] OJ L218/8.
[250] *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters* [2014] OJ L130/1.
[251] *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)* [2016] OJ L119/1.
[252] *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* [2016] OJ L119/89.
[253] *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* [2016] OJ L194/1.
[254] There are three exceptions. "The UK and Ireland are entitled to decide not to take part in adoption of measures proposed pursuant to Title V ['Area of freedom, security and justice'] of Part Three of the TFEU [*Treaty on the Functioning of the European Union*]. (…) Denmark is exempt from all policy and criminal law measures adopted after the entry into force of the Treaty of Lisbon [i.e. 1 December 2009]. Unlike the UK and Ireland, it is not permitted to opt in to specific individual measures either at the time of adoption or a later date." (Summers et al., *The Emergence of EU Criminal Law*, 54–56)
[255] Klip, *European Criminal Law*, 197–98.
[256] Ibid., 243.

throughout the EU.[257] "The legislative practice … in implementation show a wide variety of techniques, even within one Member State. Union law leaves Member States free in the use of these techniques. It is the result that counts."[258] But all provisions must be completely implemented before deadline. The Court of Justice of the European Union (CJEU) in Luxembourg ensures that the Member States comply with their obligations and that EU law is uniformly interpreted and applied.[259]

At the CoE level, the Cybercrime Convention Committee (T-CY) facilitates the implementation of the Budapest Convention, while the Cybercrime Programme Office (C-PROC) assists state parties in their capacity building. Also worth noting is the Octopus Cybercrime Community's country wiki whose profiles provide a worldwide overview of national policies on cybercrime and electronic evidence.[260]

Before concluding, we need to mention the authorities that enforce the law. "Enforcement takes place on multiple areas and levels, meaning that there is a large variety of authorities charged with the preventing, deterring and investigating cybercrime instances. Starting at local level with local, central police forces, national special units going to European and international organisations. (…) These actors may be involved in Network and Information Security (NIS), law enforcement and defence in cyber incidents and attacks."[261] The table below shows the European stakeholders involved in cybercrime prevention, investigation, and enforcement.

In conclusion, we want to stress the ever-changing, fragmented nature of the fight against cybercrime, not only in the 'justice' dimension, but also in the 'security' dimension: "1. The landscape is constantly changing, adapting to recent developments and needs. Meaning that not only the nature of the crimes and technologies change, but also policies, best practices and players in the field. Yesterday's policies may no longer be up to date and responsibilities may have shifted to other authorities. 2. There is fragmentation as regards legislation and policies as well as regards actors involved … as cybercrime requires regulation on all levels. Cybercrime affects multiple areas of law and regulation, policies and enforcement are necessary on all levels: local, regional, national as well as international action and regulation are required."[262]

Actors involved in cybercrime prevention, investigation, and enforcement[263]			
	In NIS[264]	In law enforcement[265]	In defence
At national level	- NIS competent authorities - CERTs[266]	- Police forces - Cybercrime units	- Defence and security agencies
At the EU level	- ENISA[267] - CERT[266]-EU - EP3R[268]	- EC3 (Europol)[269] - CEPOL[270] - Eurojust[271]	- EEAS[272] - EDA[273]

[257] E.g. *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 2011/93/EU*, Brussels 16.12.2016, COM/2016/0871 final. All the measures taken are published online in EUR-Lex under the 'National transposition' tab.
[258] Klip, *European Criminal Law*, 243.
[259] Ibid., 133.
[260] Octopus Cybercrime Community: http://www.coe.int/en/web/octopus/countries
[261] 'E-CRIME D-3.2', 56.
[262] Ibid., 67.
[263] This figure is adapted from Ibid., 57.
[264] NIS: Network and Information Security.
[265] Here, 'law enforcement' is to be understood in a broad meaning that includes any entity who enforces the law.
[266] CERT: Computer Emergency Response Team (alias CSIRT: Computer Security Incident Response Team).
[267] ENISA: EU Agency for Network and Information Security.
[268] EP3R: European Public-Private Partnership for Resilience.
[269] EC3: European Cybercrime Centre at Europol (which is the EU's law enforcement agency).
[270] CEPOL: EU Agency for Law Enforcement Training (*Collège européen de police*).
[271] Eurojust: EU's Judicial Cooperation Unit.
[272] EEAS: European External Action Service, i.e. the EU's diplomatic service.
[273] EDA: European Defence Agency.

A3.2 Challenges and Controversies

Having seen what the current legal situation is regarding cybercrime in the EU, we will now focus on what it should and could be. We will try and give an overview of the main challenges and controversies.

A3.2.1 Current and Future Challenges

Two recent EU projects have made a significant contribution in identifying and addressing challenges in the cybercrime area.[274] According to the CyberROAD 'Social, economic, political and legal landscape report', "[i]nternational cooperation against cybercrime is difficult for four, partly related reasons: a) due to sovereignty protection of states, b) national security concerns, c) differences of the societal, cultural and legal background of countries and d) general weaknesses in implementation."[275]

Moreover, "[t]here is currently a range of emerging research issues related to the governance of cybercrime, mainly relating to a) the definition, focus and costs related to cybercrime, b) the reasons for convergence and divergence in regulating and governing cybercrime, c) increasing exchange with non-state actors and d) the development of legal and other normative perspectives on cybercrime":[276]

a) Cybercrime still needs to be clearly defined and classified, ranging "from stalking to pornography, from malware to espionage, from loss of personal data to threats to critical infrastructure."[277] We also lack reliable statistics on cybercrime and its damage, including direct and indirect costs.
b) International harmonisation would benefit from analysing the reasons for the convergence and divergence of cybercrime regulation in various countries, in particular by identifying "which areas are more likely to converge than others."[278]
c) Non-state actors like companies and non-governmental organisations raise awareness regarding crime and implement cybercrime regulations. Future research could analyse how the public-private interaction can be facilitated and which problems of implementation are to be expected.
d) As criminalisation "is only one way of including normative standards [see e.g. the IRPC Charter[279]] (…) more research on legitimate and illegitimate activity in cyberspace would be beneficiary [sic] to gain a normative framework on cyberactivism, cybercrime and e-democracy."[280]

From another perspective, the CAMINO 'Comprehensive roadmap (research agenda) for fight against cybercrime and cyberterrorism' sets out ten general objectives in the regulatory dimension:[281]

A. Investigatory powers in intra-jurisdictional and trans-border cases
1) Reducing the gap between the average efficacy of investigations in 'real-world' enquiries and cyber-enquiries by adequate investigatory powers
2) Finding an effective, fundamental rights-compliant framework for the future of data exchange between national and EU law enforcement authorities
3) Improving the efficacy of investigatory powers beyond the EU borders (cybercrime and money laundering)

B. Civil and criminal courts forensics, admissibility and evidential standards
4) Homogeneity and European consensus of the admissible forensic analysis process for digital evidence
5) Adaptation and updating the current legislation to the cyber and digital world

[274] See also United Nations Office on Drugs and Crime, 'Comprehensive Study on Cybercrime'. On the specific issue of a European data exchange framework for electronic evidence, there is the EVIDENCE project, too.
[275] 'CYBERROAD D-3.1', 42.
[276] Ibid., 44.
[277] Ibid., 45.
[278] Ibid., 46.
[279] Internet Rights & Principles Coalition, 'The Charter of Human Rights and Principles for the Internet'.
[280] 'CYBERROAD D-3.1', 47.
[281] Cf. Choraś and Kozik, *CAMINO Roadmap*, 56–70.

6) Coordination of the future evolution of citizens' rights protection with the adoption of new evidential standards
7) Digital forensics training and certification schemes

C. Electronic identity and trust services for data protection across borders

8) Agreement on levels of authentication
9) Alignment of public/private eIDAS[282] levels within EU
10) International management of interoperability.

Finally, here is Prof. André Klip's insight[283] on the evolution of European criminal law in cyberspace:

- "The changes brought about by new computer and telecommunication technologies to our society are enormous and, although they are ongoing, it is not an exaggeration to state that they have had and will continue to have dramatic consequences for all aspects of criminal law and criminal procedure."[284]
- "Furthermore, new legal questions are appearing on the horizon with regard to investigations into crimes committed in the information society. (…) Cloud computing raises the question of where data are stored and which legislation applies. Wireless communication also poses new problems to law enforcement agencies because the transmission of data may involve various states or international organisations."[285]
- "Even though it may be fully justified to state that cybercrime is a problem of a scale that is beyond the European Union only, this does not mean that no answer must be formulated to the question of what the European Union's approach to cybercrime is."[286]

Nevertheless, all these legal challenges should not make us forget that cybercrime "cannot be viewed in one single dimension. Only an interdisciplinary and integrated approach to the phenomenon will enable its full comprehension and allow appropriate preventive and reactive measures to be taken; the effectiveness of these measures will depend on their completeness and consistency."[287]

A3.2.2 Controversies on EU Criminal Policy

As we will see, the EU's intervention in criminal law causes controversy. A comprehensive inventory of all controversies would be tedious, so we will limit ourselves to outlining the main issues raised. A detailed discussion on criminalisation, harmonisation, and Europeanisation can already be found elsewhere[288], but these three keywords sum up the general debate. First, is criminal law required? Are criminal sanctions really necessary and efficient to address the problems? Or is there "an over-reliance on the magic of the criminal law"?[289] Second, why harmonise criminal law at the EU level? And how to do so in a coherent way while respecting the national identities of the Member States?[290] In particular, is harmonisation possible without defining 'general part' principles?[291] Third, will EU criminal law competence continue to grow in the future? How far will the legal integration process go despite resistance among Member States?

[282] Concerning *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* [2014] OJ L257/73.
[283] He is Professor of criminal law, criminal procedure and transnational criminal law at Maastricht University.
[284] Klip, *European Criminal Law*, 538.
[285] Ibid., 539.
[286] Ibid.
[287] Ghernaouti-Hélie, *Cyber Power*, 290.
[288] Summers et al., *The Emergence of EU Criminal Law*, 271–84.
[289] Ibid., 279.
[290] Cf. Art. 4 para. 2 TEU (*Treaty on European Union*): "The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government."
[291] Such as the notions of intention, participation (aiding and abetting, instigation, incitation), and attempt.

In 2009, a group of criminal law scholars issued their first manifesto on substantive law.[292] They advocate a balanced and coherent EU criminal policy based on six fundamental principles: 1) the requirements of a legitimate purpose; 2) the *ultima ratio* (or last resort) principle; 3) the principle of guilt (*mens rea* or guilty mind); 4) the principle of legality and its three subprinciples[293]; 5) the principle of subsidiarity; 6) the principle of coherence[294]. Using these principles as guidelines, they examine many EU legal acts before concluding: "[a]lthough the line to unbearable consequences has not been crossed some alarming tendencies must be observed and not be ignored: criminal law must not be adopted without pursuing a legitimate purpose; the principle of ultima ratio must not be neglected; the Member States must not be obliged to pass imprecise national criminal laws; the legislation must not answer every social problem with passing increasingly repressive acts and consider this as a value in itself."[295]

In 2013, the same 'European Criminal Policy Initiative' published a second manifesto on procedure law.[296] For these scholars, "the laws of criminal procedure and mutual legal assistance, which recently have increasingly been shaped by Union legislation, must adhere to the highest standards of the rule of law and must continuously guarantee fundamental rights, notwithstanding the fact that in this area of law various interests of states, societies and individuals have to be balanced."[297] They express six demands to the EU legislator: 1) limitation of mutual recognition[298], 2) balance of the European criminal proceeding[299]; 3) respect for the principle of legality and judicial principles in European criminal proceedings[300]; 4) preservation of coherence; 5) observance of the principle of subsidiarity[301]; 6) compensation of deficits in the European criminal proceedings[302]. With respect to these demands, as shown with many examples from EU legislation, "considerable efforts still need to be taken in order to make the Union a genuine area of freedom, security and justice with regard to criminal prosecution."[303]

A3.2.3 Specific Controversies on Cybercrime

As already noted, the definition and classification of cybercrime are still debated. In 2007, the EU Commission defined 'cyber crime' (in two words) as "criminal acts committed using electronic communications networks and information systems [in short: electronic networks] or against such networks and systems" and identified three categories: 1) traditional forms of crime committed over electronic networks; 2) the publication of illegal content over electronic media; 3) crimes unique to electronic networks, i.e. attacks against information systems, denial of service and hacking.[304]

These three categories correspond to those of the *Convention on Cybercrime*, namely "computer-integrity crimes (where the computer is object of the offence), computer-assisted crimes (where the com-

[292] European Criminal Policy Initiative, 'Manifesto I'.
[293] 1) The *lex certa* requirement (legal certainty); 2) the requirements of non-retroactivity and the principle of *lex mitior* (milder law); 3) *nulla poena sine lege parlamentaria* (no penalty without a law).
[294] Coherence must be attained both horizontally, i.e. within the legal order of the Union, and vertically, i.e. in the Member States' systems of criminal justice.
[295] European Criminal Policy Initiative, 'Manifesto I', 715.
[296] European Criminal Policy Initiative, 'Manifesto II'.
[297] Ibid., 430.
[298] Through the rights of the individual (suspect, victim or third person), through the national identity and *ordre public* (public policy) of the Member States, and through the principle of proportionality.
[299] Warning against a possible shift in power solely in favour of the prosecution, they suggest creating supranational institutions that strengthen the position of the affected individuals.
[300] There is a need for a clear set of rules governing which Member States may exercise criminal jurisdiction.
[301] EU action may only be taken on the condition that the goal pursued a) cannot be reached as effectively by measures taken at the national level, and b) due to its nature or scope can be better achieved at Union level.
[302] Safety mechanisms should include compensation measures to ensure that the first five demands are met.
[303] European Criminal Policy Initiative, 'Manifesto II', 446.
[304] *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a general policy on the fight against cyber crime*, Brussels 22.5.2007, COM/2007/267 final.

puter is an instrument), and content-related crimes (where the computer network constitutes the environment of the crime)."[305] Globally, there are more controversies on the last two categories than on computer-integrity crimes (or 'hard-core cybercrime'[306]). For brevity, we will now try and summarise the different views on criminalisation in four significant areas of cybercrime: spam and piracy (two computer-assisted crimes), child pornography and terrorism (two content-related crimes).[307]

First, 'spam' refers to unsolicited commercial email (UCE).[308] *Directive 2002/58/EC*[309] illustrates the "importance of balancing the economic interests of businesses with the privacy interests of the consumer."[310] Following the controversial 'soft opt-in' approach, direct email marketing is only allowed to subscribers who have given their prior consent, with the exception of existing customers concerning own similar products or services (Art. 13).[311] But filtering techniques have proven more helpful against spam than the threat of criminal sanctions. "While tempting, there is little evidence to support this assertion that higher penalties or criminal law sanctions actually have a dissuasive effect upon spammers."[312] Moreover, "the majority of spam in EU countries, approximately 90 per cent, is sent from outside the EU. (…) As such, the EU regime is only applicable to a very small proportion of offenders. (…) Most accept that the recent decrease in spam is borne of the increasing success of technical, rather than legal, protection measures. Technical solutions have proved most effective in providing protection against spam. (…) Rather than disparate states across continents, they rely upon the self-regulation of a few major IT players and ISPs who mostly share the interest in combating spam."[313]

Then, 'piracy' refers to copyright violations.[314] Copyright protection on the Internet is a huge challenge: how to enforce intellectual property rights (IPRs) when their infringements are so widespread? Whereas some would like to reduce or even abolish copyright, rights holders strive to strengthen copyright and enforce it by all means, including through the criminal law. "[D]ifficult questions arise as to the correct balance to be achieved between protecting the rights of the right holder, on the one hand, and protecting other interests such as the internal market or individual rights, such as freedom of information, on the other. (…) In addition, … copyright protection in the digital age cannot be divorced from matters such as 'Internet freedom' not least because there is considerable potential for obligations to be placed on Internet subscribers or Internet service provider (ISPs) to ensure that Internet connections are not used to infringe intellectual property. (…) In short, as soon as the focus moves away from commercial activities and towards the practices of individuals, the criminalisation of copyright infringement becomes controversial."[315]

More generally, content regulation is a controversial subject.[316] "The determination of what constitutes 'criminal' as opposed to 'lawful' content depends to a large extent on the political and cultural context in which issues such as censorship, freedom of expression and more broadly the relationship between the individual and the government are determined."[317] EU policy distinguishes between harmful content

[305] Koops and Robinson, 'Digital Evidence and Computer Crime', 129–30. In a way, the content of the *Cybercrime Convention* reflects the international consensus on cybercrime law (e.g. which offences are defined or omitted).
[306] Ibid., 130–32.
[307] These four areas of cybercrime are particularly relevant and instructive with respect to fundamental rights.
[308] Cf. Summers et al., *The Emergence of EU Criminal Law*, 199–230.
[309] *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)* [2002] OJ L201/37.
[310] Summers et al., *The Emergence of EU Criminal Law*, 218.
[311] What's more, each message should give the opportunity to unsubscribe (as in the 'opt-out' approach). Note that regulating spam can be seen as limiting free speech and thus interfering with the freedom of expression.
[312] Summers et al., *The Emergence of EU Criminal Law*, 227.
[313] Ibid., 228–29.
[314] Cf. Ibid., 113–55.
[315] Ibid., 119.
[316] Cf. Ibid., 156–98.
[317] Ibid., 156.

and illegal content. "Illegal content is considered obviously and universally unlawful, whereas the decision about whether content is 'harmful' or not is considered to depend on 'cultural differences'…"[318] But even illegal content stirs controversy. "Some offences, notably those relating to child pornography, are widely accepted as necessary even though questions remain as to their scope, while others, such as some of the provisions on terrorist offences are the subject of considerable controversy both as regards their desirability in the first place and their extent."[319]

Directive 2011/93/EU defines a child as any person below the age of 18 years[320], although young people under 18 already have sexual consent in all EU countries except Malta. Child pornography includes "not only pornographic material involving actual children, but also pornographic material involving adults who look like children (youthful adult pornography) and computer-generated pornographic material involving children, although not created using any actual children (virtual-child pornography)."[321] Some argue that "these broad provisions, which seem to test the boundaries of the criminal law, will nevertheless prove difficult to reconcile with constitutionally protected notions of free speech and the presumption of innocence. (…) 'The emphasis shifted from protecting children from harm to attacking possession itself.'"[322] Others question the legal certainty of youthful-adult pornography. "Whether or not a person of age appears as a minor cannot be described legally. (…) This criterion will not lead to foreseeable results and is not suitable for the use in criminal law provisions."[323]

Finally, as for terrorism, "[t]he Internet is referred to as having the potential to 'inspire and mobilise local terrorist networks and individuals' and as a source of 'information on terrorist means and methods' such as amount to a 'virtual training camp'."[324] *Directive (EU) 2017/541*[325] includes the 'public provocation to commit a terrorist offence' among offences related to terrorist activities (Art. 5). This offence "has been subject to considerable criticism both because of its wide scope and because of uncertainty about the commitment to fundamental human rights guarantees, notably freedom of expression. The definition of 'terrorist offence' is undeniably broad and this breadth is expanded further by the definition of provocation which does not require that the speech actually results in a terrorist act, only that the speech 'causes a danger' that an offence may be committed."[326] However, in this area "the focus of the EU has been very much on holding individual users liable rather than on imposing liability on service or host providers. This is partly a consequence of worries about allowing governments to censor the Internet and partly due to the practical and financial burdens that would accompany demands that providers monitor all content before it is posted."[327]

A3.3 Integration of EU values

In this final section, we will consider the values at stake in criminal justice. If all of cybersecurity should be value-driven, what does it imply in the fight against cybercrime? Since our approach here is a legal one rather than an ethical or empirical one, we will focus on the values enshrined in the law.

[318] Ibid., 162.
[319] Ibid., 168. Again, regulation in these areas can be viewed negatively as limiting the freedom of speech.
[320] In accordance with the Lanzarote Convention (see § 3.1.3 above).
[321] Summers et al., *The Emergence of EU Criminal Law*, 179.
[322] Ibid., 181.
[323] European Criminal Policy Initiative, 'Manifesto I', 713.
[324] Summers et al., *The Emergence of EU Criminal Law*, 168.
[325] *Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA* [2017] OJ L88/6.
[326] Summers et al., *The Emergence of EU Criminal Law*, 172.
[327] Ibid., 175.

A3.3.1 The Legal Values Behind Offences and Penalties

Criminal offences exist to protect our legal values, by aiming to deter and punish attacks against these very values. Furthermore, criminal sanctions reveal what we value most: the more severe the sanction for an offence is, the more important the corresponding value (normally) is. For example, if the penalty for homicide is more severe than for theft, it is because human life is deemed more valuable than private property.[328] Indeed, theft is less serious than homicide[329] due to different underlying values.

Looking back, we see that criminal offences and associated penalties change over time, depending on (among others) the evolution of mores in our societies: new offences appear whereas others disappear and the definition of criminal conduct can be either expanded or narrowed.[330] Likewise, criminal law varies in space: while many offences exist in all Member States due to common European values, some offences are specific to certain countries or have more or less severe penalties across the EU.[331]

Criminal sanctions evolve, too: not only the penalties corresponding to specific offences, but also the range of sanctions itself. All CoE members (except Russia) have ratified ECHR Protocol No. 6 abolishing the death penalty.[332] "No-one shall be condemned to such penalty or executed" (Art. 1), at least not in time of peace (Art. 2). Without capital punishment, criminal sanctions now include imprisonment, fines and community service.[333] If criminal offences are defined to protect legal values, associated penalties can be seen as affecting some of the same values. Nowadays in the EU, criminal sanctions can harm a convicted person's freedom or private property, but not his/her life or physical integrity. Why is it so and not the other way around? Again, this legal situation reveals much about our underlying values.

All the crimes under EU law can be categorised according to the various legal values that they protect, namely fair competition, the integrity of the financial sector, the financial interest of the Union, human dignity, the democratic society, the integrity of public administration, public health, the fair administration of justice, the environment and, last but not least, the information society.[334] This does not mean that these EU crimes are more important than, for example, murder or rape. They simply cover the area of competence that Member States have delegated to the Union under the Lisbon Treaty.[335]

Ultimately, regardless of offences, criminalisation in itself is related to our democratic values. "There can be little doubt that the EU's involvement in the criminal law has a considerable symbolic dimension. By marking out various types of conduct as violating EU law, it is [sic] can be seen to be 'expressing and defining its own political identity' thereby building the 'supranational demos[336] which it is repeatedly said to lack and which is seen by many as a prerequisite to genuine legitimacy'."[337]

A3.3.2 European criminal justice and fundamental rights

Cybercrime poses a serious threat to the rule of law. If what holds offline should also hold online, then the law should be enforced in cyberspace. As for criminal justice, this implies that there should be no impunity in the cyber world. Offences should be reported and investigated, offenders identified and

[328] Of course, the severity of the sanction also depends on other factors such as intention (e.g. is the offence deliberate or accidental?) and responsibility (e.g. to what extent is the author mature and sane?).
[329] At least from a legal point of view in our Western societies nowadays.
[330] For instance, in the Swiss Criminal Code, the offence of 'adultery' (Art. 214) has been revoked in 1990 while 'incest' (Art. 213) has been maintained. As for the offence of 'bigamy' (Art. 215), it now prohibits the plurality of marriages or same-sex partnerships since 2007. These examples mirror the changes in the definition and protection of the family under Swiss law, which themselves reflect societal and political evolution.
[331] As for harmonisation, the EU usually sets a minimum-maximum sanction, e.g. a maximum penalty of at least eight years of imprisonment. In that case, each Member State can have a different minimum penalty (if any).
[332] *Protocol No. 6 to the Convention for the protection of human rights and fundamental freedoms concerning the abolition of the death penalty* [1983] ETS No.114.
[333] As noted above, we will not discuss the various functions of criminal sanctions in this paper.
[334] Klip, *European Criminal Law*, 231–38.
[335] Regarding the extent of EU competence for criminal law harmonisation, see § 3.1.2 above.
[336] 'Demos' means the people, the common populace of a state (like in ancient Greek city-states).
[337] Summers et al., *The Emergence of EU Criminal Law*, 283.

prosecuted. Besides, citizens should trust the justice system and not take the law into their own hands. Victims should not seek to avenge themselves by fighting back against attackers in cyberspace.

Our goal here is not to discuss how and why reality departs from this ideal, but to look into the values at stake and their dynamics. Once again, we will concentrate on the values enshrined in European law. Apart from national constitutional provisions, the two main sources of fundamental rights are the ECHR[338] and the EU Charter[339]. The ECHR dates back to 1950 and has been ratified by all 47 CoE members, and therefore all 28 EU Member States. In accordance with the Lisbon Treaty (Art. 6), the EU itself shall accede to this Convention and obey its obligations.[340]

In 2009, the EU Charter became legally binding on the EU institutions and on national governments. Being now part of the EU Treaties, the Charter belongs to primary law and prevails over all other sources of EU (and national[341]) law. Every act of secondary law, e.g. a regulation or a directive, must comply with the EU Charter. However, the Charter complements but does not replace national constitutions or the ECHR. Indeed, the EU Charter applies only when a fundamental rights issue involves the implementation of EU legislation by EU institutions or by national authorities.

Regarding criminal justice, the EU Charter contains the following fundamental rights: under Title II 'Freedoms', the right to liberty and security (Art. 6), the respect for private and family life (Art. 7), the protection of personal data (Art. 8), the freedom of thought, conscience and religion (Art. 10), the freedom of expression and information (Art. 11), the freedom of assembly and of association (Art. 12), the right to property including intellectual property (Art. 17), the right to asylum for refugees (art. 18), and protection in the event of a removal, expulsion or extradition (Art. 19). Under Title VI 'Justice', the Charter includes the right to an effective remedy and to a fair trial (Art. 47), the presumption of innocence and the right of defence (Art. 48), the principles of legality and proportionality of criminal offences and penalties (Art. 49), and the right not to be tried or punished twice in criminal proceedings for the same criminal offence (Art. 50).

It is important to note that the EU Charter is consistent with the ECHR: when the Charter contains rights that come from the Convention, their meaning and scope are the same. Most of the above-mentioned fundamental rights have their counterpart in the ECHR or in one of its Protocols, which means that the case law of the ECtHR is decisive for their interpretation and application. In case of violation, legal action may be taken in national courts, in the CJEU, and ultimately in the ECtHR.

As a result, fundamental rights are well defined and doubly protected in the EU. Legal mechanisms are in place to ensure that all laws and all authorities respect these rights and freedoms. Nevertheless, the far-reaching practical implications of general principles may not be self-evident, even with the guidance of the ECtHR and the CJEU. Moreover, there can be exceptions and limitations to fundamental rights if they are prescribed by law and necessary in a democratic society, for various reasons such as the interests of national security or public safety, the prevention of disorder or crime, the protection of health or morals, and the protection of the rights and freedoms of others.

Indeed, "[s]ociety has to deal with a major contradiction that exists between the needs of justice and police investigations and the rights to the protection of privacy and freedom for individuals, corporations, government [sic], and countries."[342] Exceptions to fundamental rights seem inevitable, especially in the fight against cybercrime. For instance, solving a case often requires analysing the communications[343] of the persons involved, which interferes with the respect for private and family life as well as the protection of personal data. If all communications were recorded and stored indefinitely, these records could be useful for some investigations, but there would be serious infringements to privacy. On

[338] *Convention for the protection of human rights and fundamental freedoms* [1950] ETS No.005.
[339] *Charter of fundamental rights of the European Union* [2012] OJ C326/391.
[340] EU accession is currently under way. The EU should become the 48th party to the ECHR (without its Protocols).
[341] According to the principle of primacy (Boutayeb, *Droit et Institutions de l'Union Européenne*, 172).
[342] Ghernaouti-Hélie, *Cyber Power*, 289.
[343] Including fixed telephony, mobile telephony, Internet access, email, and VoIP (voice over Internet Protocol).

the other hand, if absolutely no communication could be traced or monitored, many inquiries would be affected.

In 2006, the EU adopted the *Data Retention Directive*[344] concerning the retention of traffic and location data for the purpose of investigation, detection and prosecution of serious crime (Art. 1). This Directive did not apply to content data, i.e. the communications themselves, but only to metadata, i.e. information about their source, destination, date, time and location (Art. 5). EU communications providers were required to store such metadata for periods of not less than six months and not more than two years (Art. 6). Thus, specific metadata could only be accessed if a competent authority requested them in time.[345] But unless service providers received a wiretapping order, they were not allowed to retain content data, which therefore could not be investigated retroactively.[346]

The *Data Retention Directive* illustrates the trade-off between crime investigation needs and privacy protection. This Directive seemed balanced but, in 2014, it was declared invalid for violating the EU Charter. For the CJEU, it "entails an interference with the fundamental rights of practically the entire European population because it concerns all persons and all means of electronic communication. (…) [Therefore,] the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8, and 52(1) of the Charter."[347] According to this important case law, although fighting serious crime is of the utmost importance to ensure public security, it does not, in itself, justify a data retention measure such as that established by this Directive.[348]

Nowadays, the fight against cybercrime cannot be separated from national security. "With security expanding far beyond the criminal domain, security strategies began searching for any sort of suspicious behavior or information that could potentially constitute a threat. The monitoring and surveillance of people's movements, actions, communications, and transactions, thus, have become crucial components of security responses within the EU and across the globe."[349] Blanket surveillance, e.g. through deep packet inspection (DPI), raises a similar fundamental rights issue than the *Data Retention Directive*. There is a significant difference between the restricted monitoring of some suspects with a suitable court warrant, and the indiscriminate surveillance of all citizens without specific reasons. Under which conditions does national security legitimate a limitation of fundamental rights?

In the face of global terrorism, our values are being put to the test. What if something could provide the necessary information to prevent a terrorist attack and save many innocent lives? It could be just gaining illegal access to a remote computer, or monitoring everyone's communications, or even torturing a suspect. A promising approach is to go beyond the supposed trade-off between security and privacy with a new "systemic approach to security [that] enables and promotes the simultaneous preservation of human security assets and fundamental civil and political rights."[350]

A3.3.3 Human rights in the area of freedom, security and justice

From another perspective, Klip notes the emergence of a European criminal justice system in the area of freedom, security and justice (AFSJ). "The merger of the two areas of the internal market and the [AFSJ], as provided by the Treaty of Lisbon, will bring important changes to criminal justice. (...) The gradual establishment of Union bodies and offices in the field of criminal justice demonstrates that a

[344] *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* [2006] OJ L105/54.
[345] If e.g. international cooperation took longer than that, digital evidence may have already been destroyed.
[346] As we are well aware since the Snowden revelations, the situation is very much different in the USA.
[347] Judgment of 8 April 2014, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, C-293/12 and C-594/12, EU:C:2014:238.
[348] On this issue, see also Judgment of 21 December 2016, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970.
[349] Pavone, Gomez, and Jaquet-Chiffelle, 'A Systemic Approach to Security: Beyond the Tradeoff between Security and Liberty', 232.
[350] Ibid., 239–40.

European criminal justice system is emerging. This can be seen from the establishment of Europol, Eurojust, the European Judicial Network, and the EPPO [European Public Prosecutor's Office]. (…) Looking at integration as a linear process, it might be expected that, one day, the [EU] will establish a European criminal court and that European prison facilities will have to be constructed."[351]

According to Klip, this evolution has a significant impact on fundamental rights. "If the Court continues to execute its authority in a similar way, a further retreat of national criminal law autonomy and a correspondingly greater degree of influence by Union law can be expected. (…) The Court's challenge for the coming years continues to be to establish the 'rights' components for the [AFSJ]. The time has come for European criminal law to demonstrate its utility for the accused and the victim."[352]

"In 1950, the [ECHR] was drafted in a context in which, as a rule, all facts relevant to the proceedings of citizens more or less took place within the boundaries of one specific state. This was also the case for human rights violations. In essence, when human rights violations occurred, there was only one state responsible and accountable for it.

However, the situation in modern European society of 2016 is completely different. Nowadays people travel continuously from one state to another and borders hardly play a role anymore in the life of many Europeans. Human conduct in the virtual world is difficult to localise. Likewise, Member States have developed intensive co-operation in criminal matters, in order to combat crime. For certain border areas, the majority of criminal proceedings do have a foreign element for which co-operation is necessary.

Of course, in these circumstances, human right violations may occur. States *also co-operate in the commission of violations* of the ECHR and the Charter. It is here that the intensive co-operation of 2016 does not match the division of accountability and responsibility contemplated in 1950. In many situations, the applicant will not be able to tell which state committed a violation, because it took place at a very early stage of the proceedings, when he did not even know that he was a suspect (for example, Germany gave information to France and violated [ECHR] Article 8, because there was no legal basis to obtain it)."[353]

As a conclusion, "[a] new perspective on human rights is necessary. Human rights must be ensured for individuals, regardless of whether it is a single Member State, two or more Member States, or even the European Union itself, that violates human rights. Human rights must not be ensured within the jurisdiction of a single Member State, but within the [AFSJ] as a whole. (…) On the basis of the Charter, the [CJEU] is quite clearly in a position to become the primary guarantor of human rights within the Union. What is necessary here is for the 'area dimension' of individual rights to be recognised."[354]

References

Boutayeb, Chahira. *Droit et Institutions de l'Union Européenne: La Dynamique Des Pouvoirs*. Systèmes. Paris: LGDJ, 2011.

Choraś, Michał, and Rafał Kozik, eds. *Comprehensive Roadmap (Research Agenda) for Fight against Cybercrime and Cyber Terrorism*. CAMINO Project, 2016. http://www.fp7-camino.eu/assets/files/Book-CAMINO_roadmap_250316.pdf.

'CYBERROAD D-3.1: Social, Economic, Political, and Legal Landscape Report', 31 May 2015. http://www.cyberroad-project.eu/m/filer_public/2016/05/02/d31_social_economic_political_and_legal_landscape_report.pdf.

[351] Klip, *European Criminal Law*, 539–41.
[352] Ibid., 541.
[353] Ibid., 541–42 (emphasis in original).
[354] Ibid., 542.

'E-CRIME D-3.2: Final Report on Counter-Measures Including Policy and Enforcement Responses', 31 March 2015. http://ecrime-project.eu/wp-content/uploads/2015/02/E-CRIME-Deliverable-3-2-FINAL.pdf.

European Criminal Policy Initiative. 'A Manifesto on European Criminal Policy'. *Zeitschrift Für Internationale Strafrechtsdogmatik* 4, no. 12 (2009): 707–16.

———. 'A Manifesto on European Criminal Procedure Law'. *Zeitschrift Für Internationale Strafrechtsdogmatik* 8, no. 11 (2013): 430–46.

'EVIDENCE D-3.1: Overview of Existing Legal Framework in the EU Member States', 30 October 2015.

'FIDUCIA D-9.2: Report Conceptualising and Classifying Cybercrime', 3 October 2013. http://www.fiduciaproject.eu/page/45.

'FIDUCIA D-9.3: Paper on Current Domestic and Supranational Policies on Cybercrime', 28 April 2014. http://www.fiduciaproject.eu/page/45.

Ghernaouti-Hélie, Solange. *Cyber Power: Crime, Conflict and Security in Cyberspace*. EPFL Press, 2013. http://www.epflpress.org/product/51/9782940222667.

Internet Rights & Principles Coalition. 'The Charter of Human Rights and Principles for the Internet'. Accessed 13 December 2016. http://internetrightsandprinciples.org/site/wp-content/uploads/2014/08/IRPC_Booklet-English_4thedition.pdf.

Klip, André. *European Criminal Law: An Integrative Approach*. 3rd edition. Cambridge: Intersentia, 2016.

Koops, Bert-Jaap, and Tessa Robinson. 'Cybercrime Law: A European Perspective'. In *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd edition. Waltham, MA: Academic Press, 2011.

Pavone, Vincenzo, Elvira Santiago Gomez, and David-Olivier Jaquet-Chiffelle. 'A Systemic Approach to Security: Beyond the Tradeoff between Security and Liberty'. *Democracy and Security* 12, no. 4 (1 October 2016): 225–46. doi:10.1080/17419166.2016.1217776.

Summers, Sarah, Christian Schwarzenegger, Gian Ege, and Finlay Young. *The Emergence of EU Criminal Law: Cybercrime and the Regulation of the Information Society*. Oxford: Hart Publishing, 2014. http://www.bloomsburycollections.com/book/the-emergence-of-eu-criminal-law-cybercrime-and-the-regulation-of-the-information-society.

United Nations Office on Drugs and Crime. 'Comprehensive Study on Cybercrime'. Draft, February 2013. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Annex 4: Cybersecurity, Privacy and Data Protection*

This annex addresses cybersecurity from the perspective of the European data protection framework. Thereby, the current legislation on European level as well as the future framework on the basis of the European data protection reform are taken into account.

A4.1 The European Data Protection Framework Addressing Cybersecurity

To understand the relation between data protection, privacy and cybersecurity, it is important to recognize the core requirements to protect personal information of individuals, as manifested in the current as well as in the upcoming legal framework.

The European Union initially regulated the processing of personal data in 1995, with the adoption of Directive 95/46/EC[355]. This directive has set the minimum standards for the protection of personal data for the EU member countries, which were obliged to transfer these into their national data protection law. However, it is not applicable for processing operations concerning public security, defence, state security, and the activities of a state in areas of criminal law. Therefore, personal data processing in the areas of police and justice is not covered by the provisions of the Directive, which has led to the emergence of a regulatory patchwork for various application scopes, such as the Council Framework Decision 2006/960/JHA[356], the 2008 Prüm Decision[357], Council Framework Decision 2008/977/JHA[358], or the Council Decision 2009/371/JHA[359]. In sum, at the moment the European Union lacks a comprehensive data protection framework which effectively covers all areas in which the protection of individual's personal information is needed.

Nonetheless, the current framework builds upon the historic foundation of Article 8 European Convention of Human Rights (ECHR), which recognises every individual's right to privacy as fundamental right. Therein, the European data protection law assumes personal information of individuals as in need of specific protection, which also involves the protection from cybersecurity risks.

* This section has been written by Eva Schlehahn (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein).

[355] *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*.

[356] *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*.

[357] The so-called Prüm decision (or Schengen III agreement) is an international agreement of 27 May 2005 which was initially concluded between Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain in Prüm in Germany. Its purpose is the regulation of cross-border cooperation and information exchange to prevent and investigate crime. While the agreement is open to all members of the European Union, only 14 have signed the agreement so far. On February 15th 2007, the justice and interior ministers of the EU member states agreed upon the integration of the Prüm provisions into EU law. Some core elements of the decision are integrated in the EU Council Decision 2008/615/JHA on 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

[358] *Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*.

[359] *Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (EUROPOL)*. This convention also contains specific provisions for the processing of information by EUROPOL of information and intelligence, including personal data (Chapter II 'Information processing system').

Directive 95/46/EC acknowledges core principles like the lawfulness of processing activities, fairness, transparency, purpose limitation and necessity, as well as the individual's rights e.g. of access and rectification. But specifically relevant in the context of cybersecurity are the responsibilities of the data controllers, namely those entities determining the purposes and means of the processing. These responsibilities include the legal obligation to effectively implement technical and organisational measures to protect the personal information they intend to collect and process.

Article 17 of Directive 95/46/EC (Security of processing) states that *'[…] the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.'* Furthermore, this article obliges to controller to carefully choose data processors acting on his behalf as well as being able to demonstrate compliance. All of these obligations aim at a level of security which corresponds to risks the personal information may be exposed to, taking into account the type processing and the nature of the data to be protected. The individually needed technical and organisational measures may vary depending on case, situation and state of the art in specific areas. Thereby, they can entail preventive as well as reactive security measures such as for example, access control, encryption, data separation, records of processing activities, technical and organisational procedures for backup and restore, or data breach notification procedures, while this list is not conclusive. Typical standards already known in classical IT security such as ISE/IEC 27001 can also be taken into account too.

In 2009, the Treaty of Lisbon brought two substantial changes for the regulation of personal data processing activities by the European Union. First, the EU Charter of Fundamental Rights[360] became binding to Member States, and the Court of Justice of the European Union (CJEU) obtained competence to enforce it. This EU Charter not only recognises a right to privacy (Article 7[361]) but also a right to data protection (Article 8[362]). Furthermore, Article 16 (1) of the Treaty of the Functioning of the European Union (TFEU) mandated the European Parliament and the Council to lay down for the protection of persona data in the areas of freedom, justice and security. So for the very first time, the Treaty of Lisbon facilitated an EU mandate for the adoption of a much more comprehensive instrument to regulate personal data processing activities for the civil sectors, as well as for the police and justice sectors. On the basis of this new mandate, the European Commission initiated a legislative process in January 2012 with the intention of harmonising the fragmented legal data protection framework across the European Union.[363] This data protection reform produced two instruments coming into force on April 27th 2016, namely the:

- *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)*[364]
- *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*

[360] Charter of Fundamental Rights of the European Union, OJ C 364, 18.12.2000, p. 1–22.
[361] Article 7 reads as follows: Everyone has the right to respect for his or her **private** and family **life**, home and **communications.**
[362] Article 8 para. 1 reads as follows: *'Everyone has the right to the **protection of personal data concerning him or her**.*
[363] Cf. COM (2012) 9 final, titled '*Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century*'.
[364] The General Data Protection Regulation (EU) 2016/679 is the main framework directly applicable in the EU member states. It is in the following abbreviated as **GDPR.**

offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[365]

Both the GDPR, as well as Directive (EU) 2016/680 are meant to apply by May 25th 2018. Furthermore, a new regulation for electronic communications is underway in the legislative process, the so-called ePrivacy regulation. It will replace the current ePrivacy Directive[366] with a possibly expanded scope including Over-The-Top providers in addition to traditional telecom operators. However, despite being a completely new legal framework, the above-mentioned core principles of the current Directive 95/46/EC remain. This includes the obligation of the controller(s) and processors to implement the appropriate technical and organisational measures to protection the personal information they intend to collect and process.[367]

Especially noteworthy are Article 32 GDPR and corresponding, Article 29 in Directive (EU) 2016/680 which manifest specified requirements to ensure the security of processing. Both articles require the controller to conduct a risk assessment. Yet, it is very important to note that while the risks assessment as known classical in IT security, the data protection perspective is very different. IT security departments e.g. of companies are used to assess risks based on which financial or reputation damage for the company could be expected. In a proper data protection based risk assessment though, the perspective of the concerned data subject is paramount. A number of aspects play a role, such as the nature, scope, context and purpose of the processing, the inherent risks of varying likelihood and severity for the rights and freedoms of the concerned data subjects, as well as the state of the art and implementation costs of the needed measures. In cases where the processing is deemed to result in a high risk to the rights and freedoms of natural persons, an additional data protection impact assessment must be conducted.[368]

Based on these assessments, the controller is required to determine the concrete technical and organisational measures needed to sufficiently protect the personal data. According to Art. 32 (2) (b) GDPR, those measures are required to ensure the confidentiality, integrity, availability and resilience More specific examples of technical and organisational measures are also made in both legal frameworks in various places, such as pseudonymization, encryption, the documentation of processing operations, access control, and logging.[369] Such measures can also be part of a data protection by design and by default approach as also demanded by the respectively applicable legal frameworks.[370]

In contrast to the currently applicable Directive 95/46/EC, non-compliance is more likely to lead to negative consequences for the controller, since the competent data protection supervisory authorities are granted increased enforcement powers by the new legal framework, including higher number frames for fines. Even though differences regarding the required timeframes until implementation are to be expected, it might be advisable for each data controller to establish organisational test and release procedures and policies for data handling as well as risk and data protection impact assessments as early as possible. This assumption is supported by the requirement of repeated review and – if necessary – update of measures stated e.g. in Article 24 (1) sentence 2 GDPR. This means that in cases where the circumstances of the processing change in some way, the original presumption of meeting the state of the art cannot serve as an argument anymore. So when considering fines, it must be assumed that the

[365] In contrast to the GDPR, the regulatory instrument for the police and justice sectors comes in form of a directive which needs to be transferred into correlating national law by the European countries. It is in the following abbreviated as **Directive (EU) 2016/680**.

[366] *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)*.

[367] See Articles 24 (1) and 28 (1) GDPR or Articles 19 (1) and 22 (1) Directive (EU) 2016/680.

[368] Article 35 GDPR and Article 27 Directive (EU) 2016/680.

[369] See for those examples in the GDPR: Articles 6 (4) e (Lawfulness of processing), 30 (Records of processing activities), while the Directive (EU) 2016/680 has in parts even more technically specific requirements e.g. for logging, access control and other security measures, cf. Articles 25 (Logging) and 29 (Security of processing).

[370] See the Articles 25 GDPR and 20 Directive (EU) 2016/680.

respectively competent data protection supervisory authorities will take into account the effort and cooperation willingness of the controller, as well as how many of the required measures are implemented.[371] Consequently, making use of yearly security checks, audits, and best practices in technology, such as penetration tests and performance indicators seem to be reasonable to demonstrate compliance.

Beyond the preventive and reactive technical and organisational measure to protect the data, controllers and processors are required to make data breach notifications under certain circumstances and within specific timeframes. According to Article 4 (12) GDPR, *'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*'. Therefore, the GDPR directly refers to security incidents with negative effect on the protection of personal data which may also play a role within the cybersecurity domain.

According to Article 33 GDPR, a notification of a personal data breach to the supervisory authority is required no later than within 72 hours, unless a risk to the rights and freedoms of natural persons is unlikely. But according to Article 34 GDPR, if there is a high risk, the notification must also be made directly to the data subject without undue delay, unless specific technical and organisational measures are in place to render the personal data unintelligible to any person who is not authorised to access it, such as encryption. Moreover, a notification may be omitted if the controller has taken subsequent measures to ward off this high risk, or if the notification would involve disproportionate effort. However, in the latter case, a public communication or similar measure may be required of the controller nonetheless.

Besides all of these above-mentioned requirements of GDPR and Directive (EU) 2016/680, a close observation of the still active legislative process for the future ePrivacy Regulation seems advisable. Since the future ePrivacy Regulation, meant to also be in force and applicable by May 2018, will be the upcoming special law for the area of electronic communications, it plays also a significant role in cybersecurity matters too. This proposed regulation will most likely still undergo changes as the draft[372] being current at the time of writing this document has been criticised significantly by relevant stakeholders in the data protection domain, such as the Article 29 Working Party[373] and the European Data Protection Supervisor. What might matter most in the context of cybersecurity and more general IT security issues, the current draft has been found faulty for vagueness in the scope definition, as well as for weakened requirements in relation to information about security risks and data breaches, as well as regarding privacy by design and by default in comparison to the GDPR and thus provides lack of consistency.[374]

A4.2 Current and Future Challenges from Data Protection Perspective

Worldwide, cybersecurity issues emerge or intensify with the further progression into the digital era. The growing use of information and communication technologies correlates with an increasing dependence on hard- and software which can be vulnerable to threats of the most different kind. This affects

[371] See Article 83 (2) (c) + (d) GDPR, directly referring to the requirements mentioned in Articles 25 and 32 GDPR.

[372] The '*Proposal for a Regulation on Privacy and Electronic Communications'* as made by the European Commission in early 2017 is available at: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

[373] The Article 29 Working Party was set up on account of Article 29 EU Data Protection Directive 95/46/EC, which demands the formation of a working group on the Protection of individuals with regard to the processing of personal data. It functions as an independent advisory group counselling the European Commission in respect to data protection and privacy issues.

[374] See the Article 29 Working Party: '*Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)*', adopted on 4 April 2017, WP247, pages 3 and 24. Furthermore, see the '*Opinion 6/2017 EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*', April 24th 2017, pages 3, 12 ff., 19, 22 f., and 34 f.

civilian as well as governmental areas alike, making appropriate responses crucial to succeed in providing the availability, integrity and confidentiality of those technologies.[375] This includes also the personal data of individuals which is being collected and processed by digital technologies, and which may be exposed to cybersecurity risks.

Cybersecurity incidents can cover a wide spectrum, ranging from e. g. hacking, blackmail encryption, data or identity theft. They can be caused by the most diverse entities for a number of different reasons, and with varying, often unforeseeable impact. With regard to cybersecurity challenges in general, the European Union Agency for Network and Information Security (ENISA) developed a taxonomy classifying different threat types and individual threats at various level of detail. The purpose of this taxonomy is to establish a point of reference in a living structure.[376] According to this document, a number of high level threat types have been identified, such as physical attacks, unintentional damage/loss of information or IT assets, disaster (natural, environmental), failures/malfunction, outages, eavesdropping/interception/hijacking, nefarious activity/abuse, and legal. A lot of these threats are closely linked to the cyber domain, for example hacking, IoT, botnets, ransomware, or doxxware.[377]

While private actors may conduct cyberattacks for monetary or social motives, governmental activities usually extend to wider dimensions, which include Law Enforcement Agency (LEA) cyberspace activities for purposes of crime investigation or prevention, as well as further intelligence activities focused on national security. The targeted entities can also be varied, whereas the attack of critical infrastructure is to be considered as the most concerning for all countries worldwide, closely followed by attacks on the governmental structures themselves, e.g. by various types of election fraud.

When focusing on governments specifically as potential cybersecurity attackers, the use of so-called surveillance-oriented security technologies (SOSTs) plays a significant role. Many states, also within the EU, allow to varying degrees and with different preconditions the deployment of such technologies[378], which is often criticised by the media and human rights activists.[379] Media reports about technology used by governments to infiltrate citizen's devices brought into discussion their inherent risks of misuse and bias, usually coming along with a severe lack of transparency.

An example is the governmental deployment of software infiltrating citizen's devices to gain access to communications and files. In Germany, a Trojan Horse malware (named '*Bundestrojaner*', translated: '*Federal Trojan*' or '*State Trojan*') was discovered by the German Chaos Computer Club (CCC) in 2011 which employed surveillance functionalities on targeted devices. The software was enabled for backdoor remote control and was proved generally weakening the security of the targeted device. The revelation of the use of this malware triggered a significant public debate around the legality of such technologies in democratic societies.[380]

Another example is the use of so-called zero-day exploit acquisition by governmental institutions to gain leverage in the field of domestic as well as foreign intelligence. Such approaches have received critical attention due to making the whole It landscape more insecure, while leaving security loopholes open

[375] This was explicitly acknowledged by the European Union in its '*Cybersecurity Strategy of the European Union - An Open, Safe and Secure Cyberspace*', JOIN (2013) 1 final, note 4, Brussels February 7th 2013, page 3.
[376] Initial version 1.0: '*ENISA Threat Taxonomy - A tool for structuring threat information*', January 2016.
[377] Ibidem, cf. pages 8 ff.
[378] See for example, Pietrosanti, F. and Aterno, S., '*Italy unveils a legal proposal to regulate government hacking*', published February 15th 2017 under: https://boingboing.net/2017/02/15/title-italy-unveils-a-law-pro.html.
[379] Cf. the report '*Dangerously disproportionate: The ever-expanding national security state in Europe*', published by the organisation Amnesty International on January 17th 2017. The report heavily criticises the digital surveillance of European governments as negatively affecting the cybersecurity of citizens' devices.
[380] German CCC publication: '*Chaos Computer Club analyzes government malware*', published October 8th 2011.

for the obtainment and potential exploitation not only by agencies with lawful national security interests, but also by malicious outsiders.[381]

Another case with similar predicament is the debate around so-called 'lawful access' of police as well as intelligence agencies. Many of such institutions have long been demanding access to encrypted devices via backdoor functionalities. Thereby, legal obligations imposed on companies to implement such might in future affect all thinkable types of software and even hardware. Furthermore, the impact of weakened encryption permeates all deployment sectors, including the financial sector due to the increasing use of cryptocurrency such as Bitcoin. Similar as with zero-day exploits, there is some risk of proliferation beyond the LEA sphere. Furthermore, the legal and factual preconditions for the access to encrypted information are not always clear, requiring clarification. Among security experts, there seems to be a growing recognition of the need to establish mandatory warrants and additional safeguards against misuse.[382] But even beyond the mere scientific area, encryption has been acknowledged as presenting a number of different challenges for the criminal justice sector. In November 2016, the Council of the European Union[383] proposed the launch of a reflection process on such challenges, led by the European Commission.[384] Encryption was then further addressed in the Council Meeting on 8th and 9th December 2016, at which the Ministers acknowledged that this is an area to be approached carefully to take into account the risks to privacy and cybersecurity.[385] Furthermore, the ENISA published an opinion paper on encryption in December 2016, coming to the conclusion that weakening encryption to enable lawful interception is not an optimal approach. The ENISA explicitly warned of unintended consequences, e.g. weakening digital signatures and recommended some further benefits and risks analysis, as well as a more in-depth exploration of alternatives before any legislative actions should be taken.[386] Similarly, the European Group on Ethics in Science and New Technologies (EGE)[387] published an opinion already in 2014 on security and surveillance technologies, highlighting the dangers of such technologies. It pointed out that while foreign state actors may pose a problem, it should not be forgotten that the deployment of intrusive surveillance technologies domestically is risky as well. Therefore, European and democratic principles and values must be taken into account carefully.[388]

Therefore, specifically in the national security context, it ultimately comes back to the question of boundaries and which goals domestic surveillance should be allowed to pursue, taking into account the

[381] A recent example is the theft of some the US National Security Agency's most powerful espionage tools by the Shadow Brokers group. These were hoarded by the NSA's TAO (Tailored Access Operations) department, yet outsiders from the mentioned hacking group published them in August 2016, causing significant media reaction. See e.g. Nakashima, E. for The Washington Post Online: '*Powerful NSA hacking tools have been revealed online*', August 16th 2016.

[382] Bellovin, S., M.; Blaze, M.; Clark, S.; Landau, S.: '*Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*', 12 Nw. J. Tech. & Intell. Prop. 1 (2014).

[383] The **Council of the European Union** is an official EU body, whose members are the ministers from each EU country, on the basis of the respective policy areas which are addressed. It should not be confused with the **European Council**, which is another EU body consisting of the 28 EU member state government leaders, the European Council President and the President of the European Commission. The European Council defines the EU's strategic short- and long-term policy agenda. For the sake of completeness, there is another entity named **the Council of Europe (CoE)**. Yet, this is not an official EU body, but a human rights organisation which was established in 1949 after World War II. It now comprises of 47 member states, 28 of which belong to the European Union. All CoE member states have signed up to the European convention on Human Rights, and the ministers of foreign affairs of each member state is involved in the committee of ministers as the decision-making body of the CoE.

[384] Cf. Note 14711/16 from the Council of the European Union Presidency to the Permanent Representatives Committee/Council on the subject title '*Encryption: Challenges for criminal justice in relation to the use of encryption - future steps - progress report*', Brussels November 23rd 2016, page 7.

[385] Outcome of the 3508th Council meeting, document 15391/16 and press release 67 by the Justice and Home Affairs department, section '*Criminal justice in Cyberspace*', Brussels, 8th and 9th December 2016, page 7.

[386] European Union Agency for Network and Information Security, '*ENISA's Opinion Paper on Encryption - Strong Encryption Safeguards our Digital Identity*', December 2016, page 5.

[387] The European Group on Ethics in Science and New Technologies is an independent advisory body of the President of the European Commission.

[388] Opinion No. 28 of the European Group on Ethics in Science and New Technologies, '*Ethics of Security and Surveillance Technologies*', Brussels May 20th 2014, p. 87 ff..

necessity and proportionality of measures.[389] This however, is not an issue reserved exclusively to the matter of backdoors in encryption, but to all governmental activities involving SOSTs. Especially with the increasing use of Big Data analysis tools by LEAs, there is much concern related to citizens having only limited possibilities to defend themselves against any mistreatment or security risks based on algorithmic-founded suspicion. The same counts not only for LEA activity in the context of specific crime prevention or investigation, but also for intelligence in the interest of national security.

Naturally, all intelligence institutions aim at being able to use IT vulnerabilities to target individuals and organisations endangering national security. However, depending on their competences and objectives, these institutions may sometimes have several, contradicting goals. For example, it appears doubtful whether both SIGINT[390] and COMSEC[391] missions can be pursued by the very same institutions without triggering unexpected internal dichotomies regarding cybersecurity issues.

Discrepancies between offensive and defensive strategies are also particularly striking with regard to any legislative acts requiring technology to generally undermine the privacy and security of citizen's computers and communications. This is evident when observing the on-going political and public debate around governments collecting personal information of their citizens. Examples are the EU-level and national controversies around data retention, counter-terrorism legislation, and the expansion of intelligence services' competences and cooperation. Combating crime and terrorism definitely plays a role in the political and legislative landscape of the European member countries. However, these on- going debates have enough impact, which can also lead to further developments of the concepts of data protection and privacy in jurisprudence. An example is Germany, where such concepts were further developed by differing between the concept of privacy and the concept of information control.[392] Already in 1983, the German Federal Constitutional Court issued its census landmark decision, which said that the principle of the informational self-determination (translated: '*Informationelle Selbstbestimmung*) is a constitutional right in itself.[393] Building on this legal history, another decision of the German Federal Constitutional Court was issued February 2008, which established a right of every citizen to have full integrity and confidentiality of his or her information technology systems (translated: '*Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*'). Due to conflict with this right, a federal law on the domestic intelligence service for the federal state North Rhine Westphalia allowing broad secret online searches of citizen's personal computers was declared unconstitutional. The court clarified that any secret online searches must occur under very strict preconditions only. This typically requires a judicial warrant and a strong indication of an imminent threat to the life, the physical integrity or the liberty of persons, or to the foundations of the state or the existence of mankind.[394] On European level, such further developments are not so evident, yet the stance of the EU with regard to citizen's fundamental rights is always subject to public scrutiny.

Cybersecurity is a matter of concern not only in the context of police and national security, or solely for EU-located state actors. Instead, it is a global issue, motivating also private actors to think about optimal cybersecurity strategies in order to mitigate risks.[395] The World Economic Forum (WEF), a Swiss non-profit foundation committed to bring business, political, academic, and other leaders together for dialogue on global, regional, and industry agendas, has also taken stance on cybersecurity. In its Global Risk

[389] Cf. Austin, L. M., '*Surveillance and the Rule of Law*', debate article published in the Surveillance & Society Journal, Vol 13, No 2 (2015), p. 298.
[390] Signals Intelligence, for example getting access to the content of people's emails.
[391] Communications Security, with the ultimate goal of protecting communications, e.g. of government officials.
[392] For the conjunction between the definitions of privacy and identity, see Rannenberg, K.; Royer, D.; Deuker, A. (ed.): '*The Future of Identity in Information Society - Challenges and Opportunities*', pp. 292 ff. (section 7.3: '*When Idem meets Ipse: The Identity of the European Citizen*').
[393] Census decision of the German Federal Constitutional Court (in German: Volkszählungsurteil Bundesverfassungsgericht) of 15th December 1983 (Az.: 1 BvR 209, 269, 362, 420, 440, 484/83).
[394] Decision of the German Federal Constitutional Court of 27th February 2008, (Az.: 1 BvR 370/07).
[395] An example is The Atlantic Council of the United States, '*A Nonstate Strategy for Saving Cyberspace*', Atlantic Council Strategy Paper No. 8, January 2017.

Report 2017, the WEF identified twelve key emerging technologies playing a role for the cybersecurity landscape of the future. There key technologies are: 3D printing, advanced materials and nanomaterials, artificial intelligence and robotics, biotechnologies, energy capture, storage and transmission, blockchain and distributed ledger, geoengineering, ubiquitous linked sensors, neurotechnologies, new computing technologies, such as quantum computing, or neural network processing, space technologies, and virtual and augmented realities.[396]

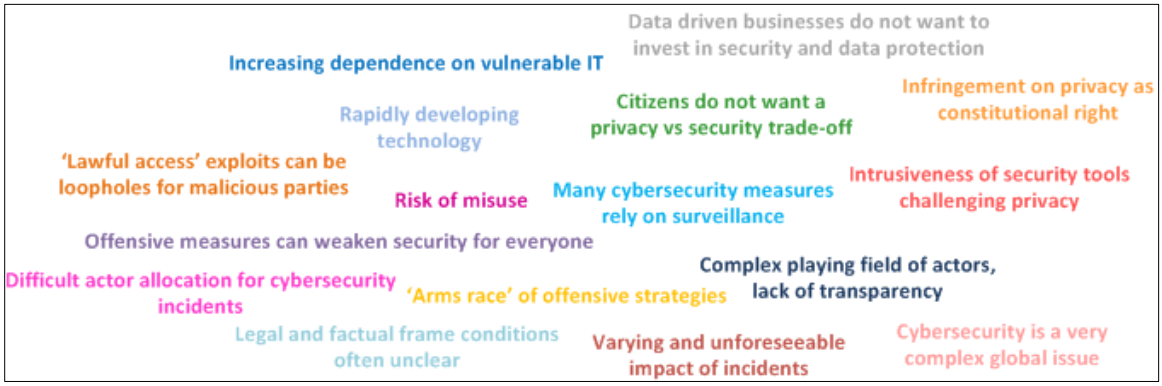

Figure A4.1: Simplified overview of cybersecurity issues

Many of such upcoming and future technologies will need adequate cybersecurity protections. Therefore, it is already foreseeable that with the growing digitalisation of the modern world, the need to address cybersecurity in an organised way will only increase.

A4.3 Cross-cutting Issues Mitigation

It becomes increasingly acknowledged that the cybersecurity issues landscape can change very fast, leaving policy-makers, data protection and cybersecurity experts at a strategical and operational disadvantage. Within the cybersecurity domain, the effectiveness of offensive measures taken mostly by governmental actors is often questioned. This is due to doubtful allocation of cybersecurity attacks and related insecurities regarding accurate forensic evidence to target the true attackers for retaliation purposes.[397] Therefore, some cybersecurity experts advise to focus more on defensive strategies in order to protect valuable assets. This is where the above-mentioned implementation of technical and organisational measures required by the current as well as the upcoming European data protection framework may also support cybersecurity in general. The responsibilities of the controller and processor entities as well as principles like data protection by design and default are focused strongly on either eliminating or at least mitigating any risks for the personal information of individuals, regardless of the type of attack. This is a considerable approach because at the moment, the cybersecurity domain provides much collaboration and information on the national level of the EU member countries, yet so far, lacks a clear, organised mandate to enforce the implementation of protective measures on European level. Nonetheless, it must be expected that with the future European data protection framework, the competent supervisory authorities will cooperate more while using their increased enforcement powers granted by the new law. So it makes sense to combine and align both the IT security and the data protection perspective because together, they can provide values as well as means to ascertain threats and

[396] Global Risks Report 2017, 12th Edition, published by the World Economic Forum within the framework of The Global Competitiveness and Risks Team, Part 3: Emerging Technologies, subchapter 3.1: Understanding the Technology Risks Landscape, p. 42.

[397] This was explicitly acknowledged by many cybersecurity experts, also abroad, see as an example the cybersecurity policy/approach of the US Obama administration, cf. Marks, Joseph: '*Obama's Cyber Legacy: He Did (Almost) Everything Right and It Still Turned Out Wrong*', January 17th 2017.

to determine mitigation measures. While addressing both security and data protection, it appears reasonable not to invent the wheel anew, but to refer to known standards and instruments like ISO/IEC 27001 and/or code of conducts as well as to process-oriented approaches (plan, do check, act). For the realisation, an effective assignment of clear responsibilities, time periods, as well as a prioritization of measures implementation should be the primary goal. To plan, implement and evaluate processes, procedures and measures in an optimal way, a data protection management system should always make clear cross-references to an eventually already existing IT security management system (ISMS) to avoid divergences, conflicts, contradictions, and unnecessary overlaps.

References

Note: URL addresses listed in the references section to point to the respective document sources originate from those which could be found on the Internet at the time of writing this White Paper, i. e. were valid links at the appointed date of August 7th 2017. No guarantee is given that those URLs still function at the time of any recipient reading this document.

Academic sources

Amnesty International (2017): *Dangerously disproportionate: The ever-expanding national security state in Europe*. January 17th 2017. Available at: https://www.amnesty.org/en/documents/eur01/5342/2017/en/

Austin, L. M. (2015): *Surveillance and the Rule of Law.* Debate article published in the Surveillance & Society Journal Vol 13, No 2 (2015). Available at: http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/viewFile/law_rule/law_rul

Bellovin, S. M.; Blaze, M.; Clark, S.; Landau, S. (2014): *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*. 12 Nw. J. Tech. & Intell. Prop. 1 (2014). Available at: http://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1

Chaos Computer Club (2011): *Chaos Computer Club analyzes government malware*. October 8th 2011. Available at: https://www.ccc.de/en/updates/2011/staatstrojaner

Marks, Joseph (2017): *Obama's Cyber Legacy: He Did (Almost) Everything Right and It Still Turned Out Wrong*. Article published at nextgov.com January 17th 2017. Available at: http://www.nextgov.com/cybersecurity/2017/01/obamas-cyber-legacy-he-did-almost-everything-right-and-it-still-turned-out-wrong/134612/

Nakashima, E. (2016): *Powerful NSA hacking tools have been revealed online*. The Washington Post Online, August 16th 2016. Available at: https://www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html?utm_term=.61735c899442

Pietrosanti, F. and Aterno, S. (2017): *Italy unveils a legal proposal to regulate government hacking*. February 15th 2017. Available at: https://boingboing.net/2017/02/15/title-italy-unveils-a-law-pro.html

The H Security blog (2012): *Federal Commissioner unable to audit Federal Trojan source*. Article published September 11th 2012. Available at: http://www.h-online.com/security/news/item/Federal-Commissioner-unable-to-audit-Federal-Trojan-source-1704460.html

Rannenberg, K.; Royer, D.; Deuker A. (ed.) (2017): *The Future of Identity in Information Society - Challenges and Opportunities*. Pages 292 ff. (section 7.3 - When Idem meets Ipse: The Identity of the European Citizen)World Economic Forum *'Global Risks Report 2017'* Insight Report, 12th Edition by the Global Competitiveness and Risks Team. Available at: http://www3.weforum.org/docs/GRR17_Report_web.pdf

Legislation

Charter of Fundamental Rights of the European Union. OJ C 364, 18.12.2000, p. 1–22. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000X1218 (01)

Consolidated version of the Treaty on the Functioning of the European Union. OJ C 326, 26.10.2012, p. 47–390. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

Treaty *of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community.* Signed at Lisbon, 13 December 2007. OJ C 306, 17.12.2007, p. 1–271. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT

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. 31-50. Available at: http://eur-lex.europa.eu/eli/dir/1995/46/oj

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, 4.5.2016, p. 1–88. Available at: http://eur-lex.europa.eu/eli/reg/2016/679/oj

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. OJ L 119, 4.5.2016, p. 89–131. Available at: http://eur-lex.europa.eu/eli/dir/2016/680/oj

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. Available at: http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32002L0058

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 386/89, 29.12.2006, p. 89-100. Available at: http://eur-lex.europa.eu/eli/dec_framw/2006/960/oj

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. OJ L 350, 30.12.2008, p. 60–71. Available at: http://eur-lex.europa.eu/eli/dec_framw/2008/977/oj

Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (EUROPOL). OJ L121/37, 15.5.2009, p. 37 – 66. Available at: http://eur-lex.europa.eu/eli/dec/2009/371/oj

Case law and policy documents

Article 29 Working Party: *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)*. Adopted on 4 April 2017 (WP247). Available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

European Data Protection Supervisor: *Opinion 6/2017 EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*. April 24th 2017. Available at: https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

High Representative of the European Union for Foreign Affairs and Security Policy: *Cybersecurity Strategy of the European Union - An Open, Safe and Secure Cyberspace.* Joint Communication to the

European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Brussels 7.2.2013. JOIN (2013) 1 final. Available at: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

Council of the European Union Presidency: *Encryption: Challenges for criminal justice in relation to the use of encryption - future steps - progress report*. Note 14711/16 to the Permanent Representatives Committee/Council, Brussels, November 23rd 2016. Available at: http://data.consilium.europa.eu/doc/document/ST-14711-2016-INIT/en/pdf

Council of the European Union - Justice and Home Affairs department: *Outcome of the 3508th Council meeting*, Document 15391/16, section '*Criminal justice in Cyberspace*' and Press release 67, Brussels, 8th and 9th December 2016. Available at: http://data.consilium.europa.eu/doc/document/ST-15391-2016-INIT/en/pdf

European Group on Ethics in Science and New Technologies: *Ethics of Security and Surveillance Technologies*. Opinion No. 28, Brussels, May 20th 2014. Available at: https://bookshop.europa.eu/en/ethics-of-security-and-surveillance-technologies-pbNJAJ14028/

European Union Agency for Network and Information Security (ENISA): *ENISA's Opinion Paper on Encryption - Strong Encryption Safeguards our Digital Identity*. Released December 2016. Available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-encryption

European Union Agency for Network and Information Security (ENISA): *ENISA Threat Taxonomy - A tool for structuring threat information*. Initial Version 1.0, January 2016. Available at: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

Non-European and national legislation, case law and policy documents

Census court decision of the German Federal Constitutional Court (In German: *Volkszählungsurteil Bundesverfassungsgericht*). 15th December 1983. Az.: 1 BvR 209, 269, 362, 420, 440, 484/83. Available at: https://cdn.zensus2011.de/live/uploads/media/volkszaehlungsurteil_1983.pdf

Court Decision of the German Federal Constitutional Court on the basic right of every citizen to have full integrity and confidentiality of his or her information technology systems (In German: '*Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*'). 27th February 2008. Az.: 1 BvR 370/07. Available at: http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html

List of Acronyms and Abbreviations

CJEU	Court of Justice of the European Union
DPIA	Data Protection Impact Assessment
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Network and Information Security
EU	European Union
GDPR	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)
LEA	Law Enforcement Agency

NIS Directive	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
NSA	National Security Agency (USA)
OJ	Official Journal of the European Communities
OJ C […]	Official Journal of the European Communities – Information and notices
OJ L […]	Official Journal of the European Communities – Legislation
SOST	Surveillance-Oriented Security Technology
TAO	Tailored Access Operations
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

Annex 5: Cybersecurity Definitions Developed by EU Member States

The table below provides an overview of cybersecurity definitions developed in national cybersecurity strategies of 18 EU Member States. While there are some similarities between the listed definitions, the variety of definitions is overwhelming as is the vocabulary invoked within them. In cases, where a strategy did not provide a definition for 'cybersecurity', we looked for definitions of the term 'cyberspace'. Some definitions suggest a more limited understating of cybersecurity, focusing on technical requirements and protection of virtual assets (e.g., the Dutch Cybersecurity Strategy), whereas others are more compressive in their scope (e.g., Slovakian, Hungarian and Czech). Luxembourg and Latvia adopted the term proposed by the International Telecommunication Union (ITU). National strategies that are listed below are available in English and can be downloaded on the website of the European Union Agency for Network and Information Security (ENISA).

#	Document title, country, year	Definition
1.	Austrian Cyber Security Strategy, 2013	The term "cyber security" stands for the security of infrastructures in cyber space, of the data exchanged in cyber space and above all of the people using cyber space.
2.	Croatian Cybersecurity strategy, 2015	Cyber security - encompasses activities and measures for achieving the confidentiality, integrity and availability of information and systems in cyberspace.
3.	Czech Republic Cybersecurity Strategy for the period of 2015-2020	Cyber security comprises a sum of organizational, political, legal, technical, and educational measures and tools aiming to provide a secure, protected, and resilient cyberspace in the Czech Republic for the benefit of both public and private sectors, as well as for the general public.
4.	Cybersecurity Strategy of the Republic of Cyprus: Network and Information Security and Protection of Critical Information Infrastructures, 2012	Cybersecurity refers to the broader security of networked systems that operate in cyberspace, i.e. in most cases connected to the Internet, and this term also covers the safe and secure usage of these systems by end users.
5.	Dutch National Cyber Security: Strategy From awareness to capability, 2014	Cyber security refers to efforts to prevent damage caused by disruptions to, breakdowns in or misuse of ICT and to repair damage if and when it has occurred. Such damage may consist of any or all of the following: reduced reliability of ICT, limited availability and violation of the confidentiality and/or integrity of information stored in the ICT systems.
6.	Estonian Cyber Security Strategy, 2014-2017	Cyber security is an integral part of national security, it supports the functioning of the state and society, the competitiveness of the economy and innovation.
7.	Finland's Cyber security Strategy, 2013	Cyber security means the desired end state in which the cyber domain is reliable and in which its functioning is ensured.
8.	Italian National Strategic Framework for Cyberspace Security, 2013	With the term cyberspace we refer to the complex of all interconnected ICT hardware and software infrastructure, to all data stored in and transferred through the networks and all connected users, as well as to all logical connections however established among them. It therefore encompasses the Internet and all communication cables, networks and connections that support information and data processing, including all mobile Internet devices.

9.	Cyber Security Strategy for Germany, 2011	Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace.
10.	Hungarian Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary, 2013	Cyber security is the continuous and planned taking of political, legal, economic, educational, awareness-raising and technical measures to manage risks in cyberspace that transforms the cyberspace into a reliable environment for the smooth functioning and operation of societal and economic processes by ensuring an acceptable level of risks in cyberspace.
11.	Cyber Security Strategy of Latvia, 2014-2018	Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.
12.	Lithuanian Cyber Security Strategy, 2011-2019	Electronic information security equates to cyber security.
13.	Luxembourg Cybersecurity Strategy, 2015	Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user assets. Organisation and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user assets against relevant security risks in the cyber environment. The general security objectives comprise the following: - Availability; - Integrity, which may include authenticity and non-repudiation; - Confidentiality.
14.	Malta, National Cyber Security Strategy, Green Paper, 2015	Cybersecurity 'is the safeguards and actions that can be used to protect cyber domain from those threats that are associated with or that may harm its interdependent networks and information infrastructure. It strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.'
15.	Cyberspace Protection Policy of the Republic of Poland, 2013	Cyberspace security – a set of organizational and legal, technical, physical and educational projects aimed at ensuring the uninterrupted functioning of cyberspace.
16.	Cyber Security Concept of the Slovak Republic for 2015 - 2020	Cyber security is one of the defining elements of the security environment of the Slovak Republic and a subsystem of national security. At a state level, *it is a system* of continuous and planned increasing of political, legal, economic, security, defence and educational awareness, also including the efficiency of adopted and applied risk control measures of a technical-organizational nature in cyber space in order to transform it into a trustworthy environment providing for the secure operation of

		social and economic processes at an acceptable level of risks in cyber space.
17.	National Cyber Security Strategy of Spain, 2013	Cyber security is a necessity of our society and our economic model.
18.	UK National Cyber Security Strategy, 2016-2021	'Cyber security' refers to the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.

Annex 5: EU values

This annex outlines European Union (EU) values listed in the EU governing treaties and it also provides a brief explanation of each value. The table below lists values included in the Treaty of the EU and the Charter of Fundamental Rights of the EU (EU Charter). The third column merges notions provided in the two legally binding documents into one list.

Treaty of the EU, Article 2	Charter of Fundamental Rights of the EU, Preamble	EU values
Human dignity	Human dignity	Human dignity
Freedom	Freedom	Freedom
Democracy	Democracy	Democracy
Equality (including equality between women and men)	Equality	Equality
Non-discrimination	The rule of law	Non-discrimination
The rule of law	Solidarity	The rule of law
Respect for human rights (including the rights of persons belonging to minorities)	Protection of individuals by establishing the citizenship of the Union and by creating an area of freedom, security and justice	Respect for human rights
Pluralism		Pluralism
Tolerance		Tolerance
Justice		Justice
Solidarity		Solidarity
		Protection of EU citizens

The descriptions below present an attempt to highlight the main aspects of EU values that are listed in EU governing treaties. It can be argued that EU values listed in the table above morphed out of the EU Member States' constitutional traditions and the fundamental rights framework, which is guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms. EU values and principles have been subject to legal scholarship and extensive case law and therefore it should be noted that descriptions provided below shed little light on the complexity of each notion. For further reading, please consult the Charterpedia webpage that was created by the European Union Agency for Fundamental Rights (FRA).[398]

Human dignity – [t]he dignity of the human person is not only a fundamental right in itself but constitutes the real basis of fundamental rights. […] It results that none of the rights laid down in this Charter may be used to harm the dignity of another person, and that the dignity of the human person is part of the substance of the rights laid down in this Charter. It must therefore be respected, even where a right is restricted.[399]

Freedoms are addressed in Chapter II of the EU Charter. This chapter encompasses Articles 6 to 19 and includes: the right to liberty and security (Article 6), respect for private and family life (Article 7), protection of personal data (Article 8), right to marry and right to found a family (Article 9), freedom of

[398] Chartapedia, available at: http://fra.europa.eu/en/charterpedia.
[399] This definition is provided by the Fundamental Rights Agency, available at: http://fra.europa.eu/en/charterpedia/article/1-human-dignity#group-info-explanations.

thought, conscience and religion (Article 10), freedom of expression and information (Article11), freedom of assembly and of association (Article 12), freedom of the arts and sciences (Article 13), right to education (Article 14), freedom to choose an occupation and right to engage in work (Article 15), freedom to conduct a business (Article 16), right to property (Article 17), right to asylum (Article 18), protection in the event of removal, expulsion or extradition (Article 19).

Democracy is one of the key requirements that has to be met in order for a country to join the EU. The European Council Conclusions presented in Copenhagen in 1993 (often referred as the Copenhagen criteria) considers democracy to be a political condition that signifies that a country 'has achieved stability of institutions guaranteeing democracy, the rule of law, human rights and respect for and protection of minorities, the existence of a functioning market economy as well as the capacity to cope with competitive pressure and market forces within the Union.'[400]

Equality is one of the general principles of EU law that was recognized in early case law of the Court of Justice of the EU.[401] This principle is enshrined in Chapter III of EU Charter. Article 20 of EU Charter proclaims that '[e]veryone is equal before the law.' This chapter includes different dimensions of equality which including gender equality (Article 23). This chapter also prohibits '[a]ny discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation' (Article 21). The underlying objectives of equality and non-discrimination principles have been further pursued in the EU secondary law such as the Equal Treatment Directive in the context of employment (Directive 2006/54/EC) and the Directive implementing the principle of equal treatment between persons irrespective of racial or ethnic origin (Directive 2000/43).

Solidarity is the term that is subject to the diverse use in different contexts. This principle aims at balancing economic (market focused) and social protection objectives in EU law and it is enshrined in Chapter IV of EU Charter.[402] Articles 27 to 34 of the EU Charter concern employment social cares contexts, such as: workers' right to information and consultation (Article 27), right to collective bargaining and action (Article 28), right of access to placement services (Article 29), protection in the event of unjustified dismissal (Article 30), fair and just working conditions (Article 31), prohibition of child labour and protection of young people at work (Article 32), family and professional life (Article 33), and social security and social assistance (Article 34), access to health care (Article 35), access to services of general economic interest (Article 36), environmental protection (Article 37) and consumer protection (Article 38).

The rule of law is one of key requirements for EU membership. While it is not specified, it implies that countries, which want to join the EU, firstly have to make sure that a judiciary branch in their country is independent, impartial and functions well. As explained on the European Commission portal: 'this includes, for example, guaranteed access to justice, fair trial procedures, adequate funding for courts and training for magistrates and legal practitioners.'[403] It also means that 'their government and its officials and agents are accountable under the law and that political leaders and decision-makers take a clear stance against corruption'.[404] Lastly, this principle entails a legislation process that is fair, efficient and transparent; laws must be concise and made available for the general public.

[400] European Council, Conclusions of the Presidency - Copenhagen, June 21-22 1993, 13.
[401] For example, see Judgment of the Court of 19 October 1977. - Albert Ruckdeschel & Co. et Hansa-Lagerhaus Ströh & Co. Contre Hauptzollamt Hamburg-St. Annen ; Diamalt AG v Hauptzollamt Itzehoe. - References for a preliminary ruling: Finanzgericht Hamburg - Germany. - Quellmehl. - Joined cases 117-76 and 16-77.
[402] Sangiovanni, A., 'Solidarity in the European Union', 33 *Oxford Journal of Legal Studies* (2013), Volume 33, Issue 2, 1 June 2013, Pages 213–241.
[403] European Commission, European Neighbourhood Policy And Enlargement Negotiations, https://ec.europa.eu/neighbourhood-enlargement/policy/policy-highlights/rule-of-law_en
[404] European Commission, European Neighbourhood Policy And Enlargement Negotiations, https://ec.europa.eu/neighbourhood-enlargement/policy/policy-highlights/rule-of-law_en

Respect for human rights scores high on the EU agenda and it is reflected in EU primary (i.e., EU Charter of Fundamental Rights) and secondary (e.g., the General Data Protection Regulation) legislation as well as in external action activities. The EU aims at mainstreaming the human rights and democratisation objectives by integrating them into negotiations on trade and cooperation agreements as well as by hosting dialogues on human rights. The latter allows determining 'possible ways of increasing […] [a concerned] country's commitment towards international human rights instruments'.[405] The EU Strategic Framework on Human Rights and Democracy 'reaffirms [EU] commitment to the promotion and protection of all human rights, whether civil and political, or economic, social and cultural'. [406] The same Strategic Framework 'calls on all States to implement the provisions of the Universal Declaration of Human Rights and to ratify and implement the key international human rights treaties, including core labour rights conventions, as well as regional human rights instruments.'[407] The EU also promotes human rights through its participation in multilateral forums such as the UN General Assembly's Third Committee, the UN Human Rights Council, the Organisation for Security and Cooperation in Europe (OSCE) and the Council of Europe.[408]

Tolerance is considered to be 'the opposite of any form of unlawful discrimination'.[409] The most elaborate definition of tolerance is provided in 1995 UN Declaration of Principles on Tolerance. According to this definition, tolerance means 'respect, acceptance and appreciation of the rich diversity of our world's cultures, our forms of expression and ways of being human. It is fostered by knowledge, openness, communication and freedom of thought, conscience and belief. Tolerance is harmony in difference. It is not only a moral duty, it is also a political and legal requirement. Tolerance, the virtue that makes peace possible, contributes to the replacement of the culture of war by a culture of peace'.[410] The UN Declaration notes that '[t]olerance is to be exercised by individuals, groups and States'. Tolerance is essential for the pluralism (including constitutional, religious, linguistic and cultural pluralism) to flourish.

The notion of justice is captured in Chapter VI of the EU Charter (Articles 47-50). This principle aims at ensuring procedural rights of individuals, in particular, the right to an effective remedy and to a fair trial (Article 47), presumption of innocence and right of defence (Article 48), principles of legality and proportionality of criminal offences and penalties (Article 49), and the right not to be tried or punished twice in criminal proceedings for the same criminal offence (Article 50). Justice in the form of impartial administration is a precondition to safeguard human rights.

Protection of EU citizens encompasses the rights of EU citizens laid down in Chapter V of the EU Charter and cooperation activities concerning the area of freedom, security and justice. Citizens' rights include: the right to vote and to stand as a candidate at elections to the European Parliament (Article 39), right to vote and to stand as a candidate at municipal elections (Article 40), right to good administration (Article 41), right of access to documents (Article 42), the right to refer to the European Ombudsman cases of maladministration in the activities of EU institutions, bodies, offices or agencies (Article 43), the right to petition to the European Parliament (Article 44), freedom of movement and of residence (Article 45), and the right to diplomatic and consular protection by any Member State, on the same conditions as the nationals of that Member State (Article 46).

[405] EU guidelines on human rights dialogues with third countries
[406] High Representative of the EU for Foreign affairs and Security Policy, Action Plan on Human Rights and Democracy (2015-2019) 'Keeping human rights at the heart of the EU agenda'.
[407] High Representative of the EU for Foreign affairs and Security Policy, Action Plan on Human Rights and Democracy (2015-2019) 'Keeping human rights at the heart of the EU agenda'.
[408] European Parliament, EU fact Sheets, http://www.europarl.europa.eu/atyourservice/en/display-Ftu.html?ftuId=FTU_6.4.1.html
[409] A European Framework National Statue for the Promotion of Tolerance Submitted with a view to being enacted by the legislators of European States.
[410] United Nations, Declaration of Principles on Tolerance, SHS-96/WS-5, 1995.