European University Institute

DEPARTMENT OF LAW

EUI Working Papers

LAW 2012/25
DEPARTMENT OF LAW

DATA PROTECTION AND THE PREVENTION OF CYBERCRIME: THE EU AS AN AREA OF SECURITY?

Maria Grazia Porcedda

EUROPEAN UNIVERSITY INSTITUTE, FLORENCE

DEPARTMENT OF LAW

Data Protection and the Prevention of Cybercrime: The EU as an area of security?

MARIA GRAZIA PORCEDDA

EUI Working Paper **LAW** 2012/25

ISSN 1725-6739

Printed in Italy
European University Institute
Badia Fiesolana
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu
cadmus.eui.eu

Abstract

Cybercrime and cyber-security are attracting increasing attention, both for the relevance of Critical Information Infrastructure to the national economy and security, and the interplay of the policies tackling them with 'ICT sensitive' liberties, such as privacy and data protection.

This study addresses the subject in two ways. On the one hand, it aims to cast light on the (legal substantive) nature of, and relationship between, cybercrime and cyber security, which are currently 'terms of hype' (and therefore it is descriptive). On the other, it explores the possibility of reconciling data protection and privacy with the prevention of cybercrime and the pursuit of a cyber-security policy (and therefore it explores causation).

As such, the subject falls in the 'security vs. privacy' debate, and wishes in particular to investigate whether it is possible to build 'human rights by design' security policies, i.e. a security policy that reconciles both security and human rights.

My argument hinges on a clarification of the term 'cybercrime' (and cyber-security), both by building on the literature – which recognises the mix of traditional crimes committed by electronic means (broad cybercrime or off-line crimes), and novel crimes possible only in the online environment (narrow cybercrime or online crimes) –and on original interpretations as far as the relationship between cybercrime and cyber-security is concerned.

I argue that narrow (or online) crimes and broad (or off-line) crimes are profoundly different in terms of underlying logics while facing the same procedural challenges, and that only narrow cybercrime pertains to cyber-security, understood as a policy. Yet, the current policy debate is focussing too much on broad cybercrimes, thus biasing the debate over the best means to tackle ICT-based crimes and challenging the liberties involved.

I then claim that the implementation of data protection principles in a cyber-security policy can act as a proxy to reduce cyber threats, and in particular (narrow) cybercrime, provided that the following caveats are respected: i) we privilege a technical computer security notion; ii) we update the data protection legislation (in particular the understanding of personal data); and iii) we adopt a core-periphery approach to human rights.

The study focuses on the European Union. The interaction between privacy and data protection and other liberties involved, as well as purely procedural issues, are outside of the scope of this research.

Keywords

Data protection, privacy, cybercrime, cyber-security, AFSJ (area of freedom, security and justice).

LIST OF ABBREVIATIONS

AFSJ	Area of Freedom, Security and Justice
CFSP	Common Foreign and Security Policy
CERTs	Computer Emergency Response Teams
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CNI	Critical National Infrastructure
CoE	Council of Europe
DDOS	Distributed Denial of Service
DOS	Denial of Service
DPA	Data Protection Authority
ECHR	European Convention on Human Rights (Convention for the Protection of Human Rights and Fundamental Freedoms)
ECJ	Court of Justice of the European Union
ECtHR	European Court of Human Rights (Strasbourg)
EDPS	European Data Protection Supervisor
EU	European Union
EUCFR	The Charter of Fundamental Rights of the European Union
FIPPs	Fair Information Privacy Principles
ICTs	Information and Communication Technologies
ISP(s)	Internet Service Provider(s)
ISS(s)	Information Society Services(s)
LEA(s)	Law Enforcement Agency(ies)
MS(s)	Member State(s)
OECD	Organization for Economic Cooperation and Development
PbD	Privacy by Design
PETs	Privacy Enhancing Technologies
PPP(s)	Private-public Partnership(s)
SCADA	Supervisory Control and Data Acquisition
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
WGCC	Working Group on Cybercrime and Cyber-security
WP29	Article 29 Data Protection Working Party

TABLE OF CONTENTS

DATA PROTECTION AND THE PREVENTION OF CYBERCRIME: THE EU AS AN AREA OF SECURITY?

*Maria Grazia Porcedda**

1. Introduction

1.1 Defining the Problem

'Security vs. privacy' is a familiar dichotomy since 9/11, when national security has been made conditional on increasing collection of personal information. The question whether measures to address security concerns should trump the permissible limitations of privacy and data protection has inspired innumerable laws, policy documents, books, articles, and blogs. Positions and nuances vary along and across the defining lines of security and human rights culture of those countries where the debate has flourished, notably the United States and its allies, such as the European Union (hereafter EU).

In general, some acknowledge the existence of the dichotomy, but consider either side so paramount as to justify the trump. Other authors focus on the risks we would incur by compressing these rights. A few have questioned the dichotomy, dismissing the importance of one of its terms. It is surprising, though, to observe the scant attempts to propose practical reconciliation of security with the respect of privacy and data protection, one example being the following:

> "We sometimes see "security vs. privacy," where the two are antagonistic. Notably, greater security can often be accomplished when security forces have greater information—raising privacy risks. […] The focus on surveillance…nonetheless captures only part of the story. In many instances we see "security and privacy," where the two are complementary. Under the standard approach to privacy protection, good security is an essential fair information practice. After all, good privacy policies are worth very little if hackers or other outsiders break into the system and steal the data. Both privacy and security share a complementary goal—stopping unauthorized access, use, and disclosure of personal information. Good security, furthermore, does more than keep the intruders out. It creates audit trails about which authorized users have accessed particular systems or data. These audit trails allow an accounting over time of who has seen an individual's personal information. The existence of accounting mechanisms both deters wrongdoing and makes enforcement more effective in the event of such wrongdoing."[1]

Indeed, 'information' or 'computer' or 'cyber' security and the connected cybercrimes are *à la page* topics in security circles, due to the relevance of Critical Information Infrastructure (hereafter CII) both to the economy and national security. Cyber-security policies are therefore being developed ubiquitously, and in the EU a consensus is emerging towards building a comprehensive strategy, which is timely for at least three reasons.

Firstly, computer security is becoming crucial due to the growing diffusion of digital devices connected online, which is increasing the systems' complexity and interconnectedness.[2] Yet, a

---

* This working paper is a revised version of Ms. Porcedda's EUI LL.M. thesis, finalised for publication within the context of the European Commission funded FP7 projects SurPRISE and SURVEILLE. The views expressed in the paper are the sole responsibility of its author and do not necessarily reflect the views of the European Commission.

[1] Peter Swire and Lauren Steinfeld, "Security and Privacy After September 11: The Health Care Example" *Minnesota Law Review* 86 n° 6 (2002): 1515-40.

[2] Ross Anderson, *Security Engineering. A guide to Building Dependable Distributed Systems* (Wiley, 2008).

growing number of studies show that computer security is not being properly implemented, and users' awareness of this fact is very low.[3] Companies may be either underestimating the implementation of adequate security measures,[4] or failing to implement them because of a lack of economic incentives (despite the negative consequences in terms of reputation of a breach of security) or of legal obligations, such as reporting security breaches.[5] This, in turn, leads to a shortage of reliable statistics.

Secondly, new ways of computing, such as cloud computing, are offering additional opportunities to perpetrate cybercrime, challenging data protection and privacy, as well as Law Enforcement Agencies' (hereafter LEAs) activities.[6]

Thirdly, the existing regulatory framework is proving inadequate. It has been said, "cybercrime is a term of hype and not a legal definition."[7] From a legal perspective, a satisfactory definition of cybercrime (and cyber-security) does not yet exist. Actually, the notion of cybercrime itself is blurred, encompassing different phenomena ranging from child abuse and cyber terrorism, through to spamming and cyber-attacks, and even identity theft and state espionage, and is often conflated with cyber-security. Such a chaotic approach contributes to undermining the production of reliable statistics, therefore the understanding of the real scale of the problem, and a proper system for reporting the crimes; cybercrime is, indeed, one of the most underreported crimes.[8]

Yet, cybercrime is a real phenomenon, and the relevance of cyber-security is such that it cannot be ignored anymore. The high impact of relating policies to 'information and communication technologies (ICTs)-sensitive' liberties, such as freedom of expression, privacy and data protection is also gaining increasing political and academic attention. Indeed, being in many cases ultimately about the data, privacy and data protection are called into question. Furthermore, some of the counter-cybercrime techniques adopted by LEAs further challenge privacy and data protection, which spurred new discussions on surveillance and the architecture of the internet.

In the EU, the most recent policy documents in the area of Freedom, Security and Justice (hereafter AFSJ) suggest developing policies which are 'in line' with privacy and data protection, hence they are consistent with the common 'security policy paradigm' in the EU. Accordingly, the political priority is to "ensure respect for fundamental freedoms and integrity while guaranteeing security,"[9] which translates into a high level of data protection and privacy. It should be noted that 'security' is also a vague concept, defined in the policy documents *a contrario*, in terms of threats "which have a direct

---

[3] Nir Kshetri, *The Global Cybercrime Industry. Economic, Institutional and Strategic Perspectives* (Springer, 2010); House of Lords, *Personal Internet Security*. Science and Technology Committee, 5th Report of Session 2006-07, 10 August 2007 and *Follow up to the Personal Internet Security Report*, 4th Report of Session 2007-08, 8 July 2008.

[4] Ibid.; Article 29 Data Protection Working Party, *Report 01/2010 on the second joint enforcement action: 'Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive,'* (WP 172), 10 July 2010.

[5] Kshetri, *The global Cybercrime Industry*; House of Lords, *Personal Internet Security*; *House of Lords, Follow up to the Personal Internet Security Report*; Anderson, *Security Engineering*.

[6] European Network and Information Security Agency (ENISA), *Cloud Computing, Benefits, Risks and Recommendations for Information Security*, November 2009; Claire Gayrel et al., "Cloud Computing and its Implications on Data Protection" (Paper for the Council of Europe's project on Cloud Computing, Namur, March; Maria Grazia Porcedda and Ian Walden. "Regulatory Challenges in a Changing Computing Environment." (Working paper for the Conference "Law Enforcement in the Clouds: Regulatory Challenges" Brussels, Belgium, February 24, 2011).

[7] Susan Brenner and Bert-Jaap Koops, ed., *Cybercrime and Jurisdiction. A Global Survey* (The Hague; TMC Asser Press, 2006), p. 9.

[8] Kshetri, *The Global Cybercrime Industry*; House of Lords, *Personal Internet Security*; House of Lords, *Follow up to the Personal Internet Security Report.*

[9] *The Stockholm Programme. An Open and Secure Europe Serving and Protecting Citizens*. OJ C 115, 4.5.2010, p. 47, p. 4.

impact on the lives, safety, and well-being of citizens,"[10] and related responses available. Threats are usually grouped in loose categories, which inform the basis of policy making in the AFSJ, and include "serious and organised crime, terrorism, drugs, trafficking in human beings and smuggling of persons"[11] as well as "cybercrime, the management of…external borders and…natural and man-made disasters."[12] The underlying values of 'security', which identify both the objects to be protected and the objectives teleologically pursued, are "promoting human rights, democracy, peace and stability."[13] Nevertheless, several policies addressing security threats (and therefore tackling the values highlighted above) adopted in the past few years, 'strike a balance between security and rights', namely by tending to restrict these rights excessively for the sake of 'security', instead of reconciling the two.

1.2 The Objective of this Research

This working paper intends to address the following question: how can a cyber-security policy in the AFSJ reconcile security and human rights, notably ICT based crime prevention & privacy and data protection?

This question can be broken down into the following sub-questions.

a. How do the pursuit of cyber-security and the protection of data and privacy (in the online environment) correlate? What are the drivers for both the pursuit of cyber-security and the protection of data and privacy (in the online environment)?
b. What regulatory changes should be made, if any, to the existing legislative framework in order to translate human rights compliant security actions (namely data protection and privacy compliant cyber-security policy) into meaningful policies?

In general, the R.Q. is a subset of the wider question whether it is possible to build an overarching policy tackling security threats that reconciles both security and human rights, notably security and privacy (data protection), or a 'human-rights-by-design' security policy, i.e. one that enhances the protection of human rights.

Therefore, the objective of this study is twofold. On the one hand, it is descriptive:[14] it aims to cast a light on the (legal substantive) nature of, and relationship between, cybercrime and cyber-security. On the other, it aims to explore the possibility of reconciling data protection and privacy with the prevention of cybercrime and the pursuit of 'cyber-security', and therefore wishes to explore causation (more privacy => more security). The project focuses on the EU. The interaction between privacy and data protection and other liberties involved are outside of the scope of this research; likewise, purely procedural issues are not the focal point of this research.

1.3 The Literature

This study wishes to take an interdisciplinary, policy-oriented approach, and is informed by two sets of – not necessarily interconnected – sources, to be fused into a coherent argument.

---

[10] Council, *Draft Internal Security Strategy for the European Union: 'Towards a European Security Model.'* 5842/2/10, Brussels, 23 February 2010, p. 3.

[11] Ibid. p. 35.

[12] European Commission, COM (2010) 673 final, 22 November 2010, p. 2.

[13] *Ibid.*, p. 4.

[14] Robert M. Lawless et al., *Empirical Methods in Law* (Aspen Publishers, 2010).

1.3.1 Primary sources (legal instruments and policy documents)

Primary sources include EU legal instruments and policy documents – and international ones insofar as they are relevant for the EU – relating to cybercrime, privacy and data protection.

As for cyber-crime and cyber-security, the necessary point of departure is the Council of Europe (hereafter CoE) Convention on Cybercrime[15] (hereafter Cybercrime Convention), which is the only international instrument on cybercrime adopted hitherto.[16] The text raises a number of substantive and procedural legal issues which are relevant for this research, since several EU Member States (hereafter MS) have contributed to its drafting, and it informs the base of EU legislation on the matter, namely the Council Framework Decision on Attacks against Information Systems.[17] This is the only comprehensive instrument on cybercrime at the EU level so far, and it is in the process of being overhauled.[18] A number of sector specific laws exist, but this research intends to focus on the general instruments only.

As far as soft law is concerned, several international *fora* and organizations in which all or most EU MS participate, such as the United Nations (hereafter UN) and the Organization for Economic Cooperation and Development (hereafter OECD),[19] are tackling the problem. Therefore, documents abound which are influential in shaping the EU policy strategy. However, in line with the scope outlined above, the study will solely focus on the EU policy documents that have marked the evolution of the cyber-security policy in the EU, with the exception of the OECD security Guidelines.

As for data protection and privacy, this study will analyse three instruments in particular.

Firstly, the Charter of Fundamental Rights of the European Union (hereafter EUCFR),[20] which explicitly draws a distinction between privacy and data protection – two related, but different, rights. Secondly, the EU Data Protection Directive (hereafter Directive 95/46/EC)[21] which, despite being designed to be technology neutral, is proving inadequate to face contemporary technical challenges, for instance cloud computing, and the increasing access to data by LEAs. Therefore, I will especially analyse the documents setting the standards for its overhaul, pursuant to the innovations of the Treaty on European Union (hereafter TEU) and the Treaty on the Functioning of the European Union (hereafter TFEU), or simply the Lisbon Treaty.[22] Thirdly, the amended Directive 2002/58[23] (hereafter e-privacy Directive), which contains important provisions relating to the integration of cybercrime prevention and data protection.

---

[15] Council of Europe, *Convention on Cybercrime*. ETS n° 105, Budapest, 23 November 2001, and its *Additional Protocol Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems*. ETS n° 189, Strasbourg, 28 January 2003.

[16] At the United Nations level, discussions to start a proper Treaty on Cybercrime failed in April 2010, due to a lack of consensus among the parties.

[17] Council Framework Decision 2005/222/JHA, OJ L 69, 16/03/2005, p. 67.

[18] European Commission, COM (2012) 10 final, 25 January 2012 and COM (2012) 11 final (General Data Protection Regulation), 25 January 2012.

[19] Other international bodies addressing cyber-security include the UN's International Telecommunications Union (ITU) and the Interpol, NATO and the G8.

[20] *Charter of Fundamental Rights of the European Union*, OJ C 364, 18.12.2000, p. 1–22.

[21] Directive 95/46/EC, OJ L 281, 23.11.1995, p. 31.

[22] *Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU)*. OJ C 83 of March 30, 2010.

[23] Directive 2002/58/EC, OJ L 201, 31.07.2002, p. 37.

This study takes into account the other instruments pertaining to the EU data protection regime, (CoE's Convention 108 and it Additional Protocol[24] as well as Recommendation 87 (15),[25] Council Framework Decision 2008/977/JHA,[26] and the Data Retention Directive),[27] and will address them insofar as they are relevant for the focus of the discussion.

Last but not least, this research will refer to the doctrinal body built by the Article 29 Data Protection Working Party (hereafter the WP29), as well as the European Data Protection Supervisor (hereafter the EDPS).

1.3.2 Secondary sources (academic literature)

As highlighted above, the EU policy documents suggest building an overarching policy tackling security threats which is "in line" with privacy and data protection. Nevertheless, the acts adopted in the past few years to tackle security challenges, often couched in terms of "striking a balance between security and rights," tend to restrict rights for the sake of security, instead of reconciling the two.

The corresponding academic debate[28] has been introduced in the opening paragraphs. It translates into the opposition, sometimes fierce, between the protectors of privacy[29] and those of security.[30] The study will build on the intermediate position, held by some scholars, that it is possible, and necessary, to reconcile the two.[31]

The underlying philosophical debate of the 'security vs. privacy' dichotomy – 'interest vs. right' or 'value vs. value' – hinges on the idea that balancing is always needed according to some weighing rule which limits one in favour of the other.[32] A reinterpretation of Alexy's theory of rights[33] leads to a different result, namely a core-periphery approach to rights, according to which the rights would have

---

[24] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.* CETS n° 108, Strasbourg, 28 January 1981; *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows.* CETS n° 181, Strasbourg, 8 November 2001.

[25] Council of Europe, Recommendation of the Committee of Ministers regulating the use of personal data in the police sector (Police Recommendation). No R (87), Strasbourg, 15 17.9.1987.

[26] Council Framework Decision 2008/977/JHA, OJ L 350, 30.12.2008 p. 60 –71.

[27] Directive 2006/24/EC of 15 March 2006, OJ L 105, 13.4.2006, pp. 54-63.

[28] Stefano Rodotà, *Elaboratori Elettronici e Controllo Sociale* (Mulino, Bologna, 1973); *Intervista su Privacy e Libertà* a cura di Paolo Conti (Laterza, 2005); "Data Protection as a Fundamental Right," in *Reinventing Data Protection?* eds. Serge Gutwirth et al. (Springer, 2009), pp. 79-80.

[29] See, inter alia, Paul De Hert et al., "Data Protection in the Third Pillar: Cautious Pessimism," in *Crime, Rigths and the EU, The Future of Police and Judicial Cooperation*, ed. Martin Maik (London: Justice, 2008) and Frank Dumortier et al., "La protection des données dans l'espace européen de liberté, de sécurité e de justice," *Journal de Droit Européen* 166 (2010): 33- 46.

[30] See, inter alia, Paul Rosenzweig, "Privacy and counter-terrorism: the pervasiveness of data Rosenzweig, Paul. "Privacy and Counter-terrorism: the Pervasiveness of Data." *Case Western Reserve Journal of International Law* 42 (2010): 625-646.; Amitai Etzioni, *How patriotic is the Patriot Act* (New York and London: Routledge, 2004); Kim Taiple, "Why Can't We All Get Along? How Technology, Security and Privacy Can Co-exist in a Digital World,' in *Cybercrime, Digital Cops in a Networked Environment*, ed. Jack M. Balkin et al. (New York University Press, 2007).

[31] See, *inter alia* "Lee Tien, Architectural Regulation and the Future of Social Norms" in *Cybercrime, Digital Cops in a Networked Environment*, ed. Jack M. Balkin et al. (New York University Press, 2007); Swire and Steinfeld, "Security and Privacy After September 11"; Mary De Rosa, "Data Mining and Data Analysis for Counterterrorism." Center for Strategic and International Studies, 2004.

[32] Giovanni Sartor, "Doing Justice to rights and values: teleological reasoning and proportionality." *Artificial Intelligence and Law*, 18 (2010): 175-215.

[33] Martin Scheinin, "Terrorism and the Pull of 'Balancing' in the Name of Security," in *Law and Security - Facing the Dilemmas*, ed. Martin Scheinin, (Florence: European University Institute Working Paper N° 11, 2009).

an inviolable core sealed in a rule and a periphery subject to permissible limitations, such as those foreseen in privacy and data protection provisions, i.e. article 8 of the CoE Convention for the Protection of Human Rights and Fundamental Freedoms[34] (hereafter ECHR) and articles 7 and 8 of the EUCFR. I will build on this approach,[35] to argue that often there is no conflict but a synergy between privacy and security. The study will also borrow from the idea that privacy is not only a right but also a collective interest (which is the case in cyber-security).[36] In general, this work builds on, and assumes, the privacy literature produced in the last decades.[37]

As for cyber-security, a flourishing literature exists on its legal, technical and philosophical aspects. Works from cyber-law and legal informatics experts[38] will provide the basis to frame the problem in legal terms, in particular to judge the abovementioned legal instruments, as well as the interaction between informatics and the law, i.e. how the area can and should be regulated, as technology can accommodate any need.[39] This will overlap with more technical contributions[40] that focus on the question "what are we seeking to prevent, and will the proposed mechanisms actually work"?[41]

The idea that technology can accommodate any needs is reflected in the philosophical acknowledgment of the existence of different definitions of 'security', which bear different moral claims and pave the way to different policy outcomes. This study will draw on the distinction made between "cyber security" and "technical computer security"[42] and build on the latter. This notion, which focuses on individual harm in various forms (property, autonomy, privacy and productivity) and calls for pre-emption, requires a preventive policy, which reinforces each individual (i.e. each node of the network).

---

[34] Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No 11 and 14*. CETS n° 005, Rome, 4 November 1950.

[35] Porcedda and Walden, "Regulatory Challenges in a Changing Computing Environment"; "Law Enforcement in the Clouds: is the EU Data Protection Legal Framework up to the Task?" in *Data Protection in Good Health*, ed. Serge Gutwirth et al. (Springer, 2012).

[36] Colin Bennett, and Charles Raab, *The Governance of Privacy. Policy Instruments in a Global Perspective* (MIT Press, 2006).

[37] Inter alia, Bennett and Raab, *The Governance of Privacy*; Rodotà, *Elaboratori Elettronici*, and *Intervista su Privacy e Libertà*; Daniel J. Solove, "'I've Got Nothing to Hide' and other Misunderstandings of Privacy," *San Diego Law Review* 44 (2007): 745; Serge Gutwirth et al. ed., *Reinventing Data Protection?* (Springer, 2009); Abraham L. Newman, *Protectors of Privacy. Regulating Personal Data in the Global Economy* (Ithaca: Cornell University Press, 2008).

[38] Inter alia, Brenner and Koops, *Cybercrime and Jurisdiction*; Susan Brenner, "The Council of Europe's Convention on Cybercrime," in *Cybercrime, Digital Cops in a Networked Environment*, ed. Jack M. Balkin et al. (New York University Press, 2007); Nir Kshetri, *The Global Cybercrime Industry*; and Jonathan Clough, *Principles of Cybercrime (*Cambridge: Cambridge University Press, 2010).

[39] Tien, "Architectural Regulation and the Future of Social Norms."

[40] Anderson, *Security Engineering*; Bruce Schneier, *Beyond Fear. Thinking Sensibly about Security in an uncertain World* (Copernicus Books 2003). Ross Anderson and Tyler Moore, "The Economics of Information Security," *Science*, 314 (2006): 610-613.

[41] Anderson, *Security Engineering*, p. 2.

[42] Nissenbaum, "When Computer Security meets National Security," in *Cybercrime, Digital Cops in a Networked Environment*, ed. Jack M. Balkin et al. (New York University Press, 2007).

1.4 Hypotheses

My argument hinges on a clarification of the term 'cybercrime' (and cyber-security), both by building on the literature – which recognises the mix of traditional crimes committed by electronic means (narrow cybercrime or online crimes), and novel crimes possible only in the online environment (broad cybercrime or off-line crimes) – and on original interpretations as far as the relationship between cybercrime and cyber-security is concerned.

My first hypothesis is that narrow or online crimes and broad or off-line crimes are profoundly different in terms of underlying logics (essentially relating to data or incidentally relating to data), while facing the same procedural challenges in terms of the volatility of the evidence requiring retention, the rules pertaining to its use and exchange. In addition, only narrow cybercrime pertains to cyber security, understood as a policy; the latter, in turn, refers to the protection of critical information infrastructure (CIIP). Yet, the current policy debate is focussing too much on broad cybercrimes (see the last G8), thus biasing the debate over the best means to tackle ICT-based crimes, leaving to the military room of manoeuvre to deal with CIIP issues; both moves lead to a further challenge to the liberties involved.

My second hypothesis is twofold:

a) the implementation of data protection principles in a cyber-security policy can act as a proxy to reduce cyber threats, and in particular (narrow) cybercrime;

b) in case the implementation of data protection is not beneficial to a cybercrime investigation, the rules pursuant to it are not at odds with the need of such investigation;

Provided the following caveats are respected: i) we privilege a technical computer security notion; ii) we update the data protection legislation (in particular the understanding of personal data); and iii) we adopt a core-periphery approach to human rights.

As for a), the obligation to adopt appropriate technical and procedural security for data protection in general, and e-privacy in particular, is a clear complement to the adoption of narrow cyber-crime preventive policies. The same could be true for the application of the principle of privacy-by-design.[43] In addition, and very importantly, the obligation to notify data breaches can trigger the incentives to adopt more stringent norms on security, thus obtaining a double objective: decreasing the incidence of breaches and increasing the reporting of crimes to LEAs, thus raising the odds of successful investigations and prosecutions. However, in the case of broad cybercrime, data protection concerns are secondary and may be (perceived as) an impediment to prevent and prosecute the crime. In this case, balancing as corrected by the core-periphery approach may be needed.

As for b), this point is very important because, while prevention can reduce the incidences of cyber-crime, it will not eliminate them. This in turn entails that investigations will have to be conducted, where data protection and privacy of the people involved are at stake. The suggestion is that meaningful data protection and procedural rules could allow LEAs to operate effectively without compressing the core of the rights. The real challenge here is the extent to which data protection can be coupled with broad cyber-crime investigations and prosecution.

I will argue that, in the case of narrow cybercrime or proper cyber-security, there is little conflict between privacy and 'security', and therefore they can be reconciled without balancing, while in the second case they may conflict, thus calling for classic balancing. The use of the core-periphery

[43] Ann Cavoukian, *Privacy by Design* (Information and Privacy Commissioner of Ontario, Canada); European Data Protection Supervisor (EDPS). *Opinion on Promoting Trust in the Infor-mation Society by Fostering Data Protection and Privacy (Opinion on Privacy By Design)*. OJ C 280, 16.10.2010, p. 1–15.

formula, though, as well as the design of better procedural rules, could in theory not lead to balancing at all.

1.5 Methodology

The methodology adopted varies in accordance with the objective pursued. "Descriptive research – research that describes the state of the world – is often quite valuable...Such description can be vital to legal decision making and policy."[44] Indeed, in order to build an argument on the relationship between cybercrime and data protection, both need to be conceptually unpacked and put in the context of a legal framework of reference. The corresponding part of this project is descriptive.

The attempt to establish a correlation between data protection rules and cybercrime prevention has clearly empirical ambitions. Unfortunately, due to scope constraints, the project can only aim at laying the theoretical foundation of the argument. In the conclusion, I will suggest how the theory could be tested empirically.

Following calls from legal scholarship toward interdisciplinary research,[45] this study builds on political science methodology, and in particular on pragmatic research design.[46] Pragmatic design "mimics the way we generate knowledge in everyday social life,"[47] and aims at generating useful knowledge, the latter intended as a social and discursive activity. In practice, pragmatic design consists in: selecting an unexplained phenomenon; singling out a particular aspect to be studied; establishing the relevant concepts, which will constitute the field of study; if this leads to sub-domains of research, choosing for each the most relevant cases to be studied. Causal relationships are not the objective, but can be the result of consistent patterns. Accordingly, after having established the relevant concepts, I will use the case of cloud computing to evaluate data protection, as a situation that tests the limits of current laws and is relevant in terms of cybercrime.

The subject of this research is one amongst the several case studies in the 'security-privacy' debate. Analysing the implementation of data protection principles in a cyber-security policy will offer either strong proof that security and privacy can practically, and not only theoretically, converge in a concrete policy; or, conversely, it will show that reconciliation of the two is not in practice possible, and balancing is therefore necessary. As such, cybercrime falls under the category of inferring/confirming theories cases,[48] disciplined configurative cases,[49] or a doubly-decisive test.[50]

---

[44] Lawless et al., *Empirical Methods in Law*.

[45] Richard A. Posner, "Legal Scholarship Today," *Harvard Law Review*, 115 (2002): 1314–26; Jan M. Smits, "Redefining Normative Legal Science," in *Methods of Human Rights Research*, ed. Fons Coomans et al. (Antwerp: Intersentia, 2009), pp. 45-58; Douglas W. Vick, "Interdisciplinarity and the Discipline of Law," J*ournal of Law and Society*, 31 (2004): 163–93.

[46] Jörg Friedrichs and Friedrich Kratochwil, "On Acting and Knowing: How Pragmatism Can Advance International Relations Research and Methodology," *International Organization* 63 (2009): 701–31.

[47] Ibid, p. 714.

[48] Arend Lijphart, "Comparative Politics and the Comparative Method," *American Political Science Review*, 65. N°3, (1971): 682-693.

[49] Harry Eckstein, "Case Study and Theory in Political Science," in Handbook of Political Science, Vol. 3, ed. Fred Greenstein et al. (Reading: Addison-Wesley, 1975).

[50] Stephen Van Evera, *Guide to Methods for Students of Political Science* (New York, 1997).

1.6 Content

This work is organised as follows. Chapter 2 reconstructs the policy of cyber-security in the EU, with the objectives of both setting a frame for the analysis of the relevant legal instruments and highlighting the main characteristics of cybercrime and cyber-security, with a view to understanding whether the latter can be integrated with privacy and data protection into a coherent policy (hypothesis 2). Chapter 3 addresses the relevant instruments in cyber-security, and discusses the concepts of cyber-crime and cyber-security; in particular, I address the first hypothesis advanced, as well as the caveat on cybercrime (caveat one).

Chapter 4 is dedicated to privacy, and in particular to the two caveats relating to it (caveats two and three). Chapter 5 – the Conclusions – try to provide an answer to the research question, and in particular to show the link, *de facto* and *de iure*, between privacy and data protection, cyber-security and cybercrime. The burden of the proof is on privacy, as it is usually seen as the obstacle to achieving greater security. After some speculation about future developments, I will provide some suggestions for an empirical test of this theoretical framework.

2. The EU Approach to Cyber-Security

2.1 Introduction

Cyber-security has an undisputable cross-border and cross-sectoral nature, and any related policy can only be transversal. Hence, the subject is complex and can be approached in different manners. In the case of the EU, which started addressing the matter around fifteen years before the entry into force of the Lisbon Treaty, the intrinsic complexity of cyber-security is magnified, because 'transversal' means 'trans-pillar.' Obviously, the pillars structure has been abolished, and the EU explicitly acknowledges the link among the AFSJ, the Internal Market area and the Common Foreign and Security Policy (hereafter CFSP):

> "A concept of internal security cannot exist without an external dimension, since internal security increasingly depends to a large extent on external security. International cooperation […] is essential. The EU's policies with regard to third countries need to consider security as a key factor and develop mechanisms for coordination between security and other related policies, such as foreign policy."[51]

Moreover, the actions undertaken following the Internal Security Strategy "will also contribute to strengthening and developing the European model of a social market economy put forward in the Europe 2020 strategy."[52] Yet, it will probably be some time before the effects of the previous institutional settings can be overcome, provided this is possible at all; indeed, Commissioner Malmstrom has recently lamented the fragmentation of the cyber-security policy.[53]

As a result, I will briefly reconstruct the EU approach to cyber-security policy since its inception, by casting a light upon the most significant of the several policy documents adopted in the last fifteen years, following a chronological order, and highlighting the initiatives and overlaps between pillars. The objective is both to build a frame for the analysis of the main legal instruments adopted in the field, analyses which will be carried out in the next two chapters, as well as highlight the main features of the cyber-security policy, with a view to appraising whether in the EU data protection and privacy prevention are, or can be, aligned with the pursuit of cyber-security.

2.2 The Initial Approach to Cyber-Security: The Spill-Over from the First to the Third Pillar

2.2.1 A market-based approach

The EU's (or, as it then was, the European Community) first approach to cyberspace hinged on its potential for the development of the internal market.[54] This is not surprising, given the institutional development of the EU.[55]

The White Paper on Growth,[56] and in particular the Bangemann Report,[57] acknowledged the delay of the EU in developing a profitable e-market vis-à-vis the United States, and highlighted the need to

---

[51] Council, *Draft Internal Security Strategy*, p. 16.

[52] European Commission, COM (2010) 673 final, p. 4.

[53] The EU Security Roundtable, *European Cyber Security Conference Shared Threats – Shared Solutions: Towards a European Cyber Security Policy* (Conference Report, 14 June 2011).

[54] Maria Grazia Porcedda, "Transatlantic Approaches to Cyber-security: the EU-US Working Group on Cyber-security and Cybercrime," in *The EU-US Security and Justice Agenda in Action*, ed. Patryk Pawlak, Chaillot Paper (Paris: EUISS, December 2011).

[55] On the subject, see Leonardo Rapone, *Storia dell'Integrazione Europea* (Roma: Carocci, 2004).

remove all obstacles hindering its pursuit. In other words, they called for the creation of all conditions favourable to the development of the users' trust, such as measures to address, or better address, computer security (i.e. encryption)[58], intellectual property[59] and privacy rights.

The Bangemann Report's recommendations sparked several legislative initiatives, mostly relating to the first pillar. These include proposals to: curb child pornography online;[60] protect intellectual property;[61] enhance taxation;[62] and advance data protection.[63] Obviously, the input for the development of data protection laws cannot be reduced to the Bangemann Report, and started well before 1994, as will be addressed in 0.

However, it is important to stress the fact that privacy and cybercrime laws were urged as complementary measures to address the problems relating to the development of the internal e-market (as a subset of the internal market). This, of course, presupposed the removal of all obstacles to the 'free flow of personal data,' which is the economic rationale for the adoption of common data protection laws. The Bangemann Report actually highlighted how Europe was a leader "in the protection of the fundamental rights of the individual with regard to personal data processing."[64]

2.2.2 The spill-over to the third pillar and the 'three-pronged approach'

More or less contemporaneously to the first legislative initiatives, the European Commission carried out a study on computer-related crime (COMCRIME), whose results were presented in 1998 to the Council. The following year, the Tampere Council recommended harmonising provisions on cybercrime. Two crucial Communications followed, COM(2000) 890 and COM(2001) 298, both of which analysed the state of the art – an online environment which had expanded well beyond the concept of an e-market - and proposed actions with a 'trans-pillar' approach. I will analyse them in sequence.

COM(2000) 890: 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime'

The Communication was published in 2000,[65] as a follow up to the COMCRIME study. To begin with, the Commission urged to distinguish between crimes against infrastructure (the physical layer) and against services (the logical layer), and criticised the approach adopted by some countries to counter cybercrime, namely a traditional criminal law stance as opposed to focusing on preventive measures.

(Contd.)

[56] Commission of the European Communities, *Growth, Competitiveness, Employment. The Challenges and Ways forward into the 21st Century. White paper*, COM(93) 700, 5 December 1993.

[57] High-Level Group on the Information Society, *Recommendations to the European Council. Europe and the global information society (The Bangemann Report)*. 26 May 1994.

[58] At the same time, they acknowledged its double-edged nature, as in the case of other measures. While stressing its desirability as a way to increase consumers' trust, and prevent unauthorized access to services, they recognized it could shield hacking, and thus urged the development of an anti-piracy legal system for companies; as well as the possibility to override encryption for national security purposes. This debate is still unresolved, and I will return to it in 3.

[59] Council Directive 91/250/EEC, OJ L 122, 17 May 1991, pp. 42-46.

[60] Council Decision 2000/375/JHA, OJ L 138, 9 June 2000, p. 1.

[61] Directive 96/9/EC, OJ L 77, 27 March 1996, pp. 20-28 and *Common Position adopted by the Council with a view to the adoption of a Directive of the European Parliament and of the Council on harmonization of certain aspects of copyright and related rights in the Information Society* (CS/2000/9512).

[62] See European Commission, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, COM (2000) 890 final, 26 January 2001.

[63] OJ L 281, 23.11.1995, p. 31, and OJ L 024, 30/01/1998 P. 0001 - 000897/66.

[64] *The Bangemann Report*.

[65] European Commission, COM (2000) 890 final.

Such criticism was based on the recognition that the Internet was (and is) not, like telephone lines, a centralized network, but a decentralized one, whose security depends on the periphery, i.e. on the end-users, for which innovation and commercialization of security technology and services are crucial. The latter encompass the development of quality software, firewalls, anti-viruses, encryption, smart cards, biometric identification, electronic signatures and role-based technologies.

As for the infrastructure, the Commission recommended to ensure it against accidents, attacks or increased traffic, whereas until then security design had been sacrificed to the needs of flexibility and responsiveness. A 'security-by-design' attitude was urged, in line with the works of the EU Information Society Technologies Programme. The Commission further stated that "the implementation of security obligations following in particular from the EU Data Protection directives contributes to enhancing security of the networks and of data processing."[66]

Indeed, Article 4 of Directive 97/66/EC obliged the provider of a publicly available telecommunications service to "take appropriate technical and organisational measures to safeguard the security of its services, if necessary in conjunction with the provider of the public telecommunications network with respect to network security" at a level appropriate to the risks presented. Then, in case of "a particular risk of a breach of the security of the network, the provider…must inform the subscribers concerning such risk and any possible remedies, including the costs involved." In addition, pursuant to article 5, national regulations to "prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised" had to be adopted.

The Commission acknowledged the lack of reliable statistics, especially in the private sector, which prevented a proper assessment of the phenomenon, as well as the lack of terminological clarity. One could distinguish between computer specific crimes, whose definitions needed to be updated, and traditional crimes perpetrated by means of computer technology, which called for improved cooperation and procedural measures.

While the Communication pointed out the lack of an EU comprehensive legislation, it highlighted the existence of other instruments indirectly addressing computer crime, such as privacy offences, content-related offences (child pornography, racist and xenophobic speech), economic crimes (unauthorized access and sabotage at the MS level), and intellectual property offences (addressed by the Directive on the Legal Protection of Computer Programs and a (then) proposal for a Directive on Copyright). Again, the Commission acknowledged that, due to the fundamental rights status of personal communications, privacy and data protection, access to and dissemination of information, "availability and use of effective prevention measures are desirable so to reduce the need to apply enforcement measures."[67]

Indeed, Article 17 of Directive 95/46/EC mandates the undertaking of "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing." Moreover, pursuant to article 24, MS have an obligation to establish sanctions in case of infringement of the provisions of the Directive. In addition, Article 16 protects the confidentiality of personal data, by prohibiting any person who has access to personal data to process them "except on instructions from the controller, unless he is required to do so by law."

The Commission then suggested concrete actions to be undertaken. It urged the adoption of programs of awareness raising (i.e. the eEurope programme) and training for LEAs. It recommended measures as diverse as the creation of hot-lines, R&D, industry and community-led initiatives, co-operation

[66] Ibid., p. 11.

[67] Ibid., p. 14.

between stakeholders (through, for instance, the creation of an EU forum) and filtering of contents. The latter, depending on the technique used, is actually one of the most privacy intrusive measures; I will address this in section 2.2. It called for international action and the adoption of non-legislative measures, including private-public partnerships (hereafter PPPs). The latter refer to the cooperation of governmental bodies, notably LEAs, with the private sector, both to investigate and prevent crimes (i.e. adopting the appropriate security measures). As for legislative measures, the Commission encouraged the approximation of substantive and procedural rules at the European level on child pornography, substantive criminal law, anonymity online and mutual recognition, beyond the standards set by the Cybercrime Convention (which was deemed to have established only minimum international harmonisation), as recommended by the Tampere Council.

The Communication made clear that all measures suggested were to respect fundamental rights' permissible limitations. The Cybercrime Convention will be also addressed in greater detail in section 2.2.

This Communication is relevant for two reasons. Firstly, it mentions all fundamental policy issues relating to cybercrime, and builds a real bridge between the then first and third pillars. Several communications followed,[68] all addressing the very same issues, as hopefully this chapter will show. Secondly, it recognizes the complementarity of data protection rules and cybercrime prevention as well as cyber-security protection, which this research tries to highlight.

The WP29, which commented on the Communication,[69] acknowledged such a balanced approach. Yet, it underlined a number of intertwined shortcomings, concerning both substantive and procedural law, and questioned the decision to use the Cybercrime Convention as the basis of EU law on the matter. As for the link between substantive and procedural law, the WP29 argued that a wide concept of cybercrime, such as the one adopted by the Commission, could have offered a wide basis for the application of intrusive forensic and evidentiary techniques. Therefore, the WP29 urged drawing a clear line between the infringements associated with computer crime, such as illegal access and interception, and those relating to the application of legislation on privacy and data protection, to avoid contradictions and overlapping, while at the same time ensuring perfect coherence, in particular for the substantive law on conduct. In addition, the WP29 worried that the simple use of information technologies for traditional forms of crime could have led to the adoption of such intrusive procedures, which would have not been used otherwise, and eventually to their widespread application.

The WP29 highlighted the contrast of such risk with the principle whereby each legal procedure, as well as international cooperation rules, should be submitted to appropriate safeguards and conditions, and that the same legal guarantees should apply to procedures employed by different bodies (i.e. Europol and Eurojust). The WP29 believed the Communication should have insisted more on preventive measures; "a general improvement in security levels would contribute to reducing the risks of any compromise to network and data security."[70]

COM (2001) 298: 'Network and Information Security: Proposal for a European Policy Approach'

The Communication 'Creating a Safer Information Society' acknowledged the need to distinguish cybercrimes against the services from those against the infrastructure; the Communication analysed here dealt with the latter. The Commission highlighted the challenges of network security, due to salient features, such as network liberalisation (networks are owned and managed by private parties),

---

[68] *Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security*. OJ C 48, 28.02.2003, p. 1-2.

[69] Article 29 Data Protection Working Party, *Opinion 9/2001 on the Commission Communication on 'Creating a safer information society by improving the security of information infrastructures and combating computer-related crime,'* (WP 51), 5 November 2001.

[70] Ibid., p. 3.

convergence of networks and information systems, and internationalisation, whereby security solutions must be shared and interoperable. The Communication intended to "develop a comprehensive strategy on security of electronic networks,"[71] as requested by the Stockholm Council of 23-24 March 2001, based on the recognition of the increasing importance of communication networks for all sectors of society, as well as for the provision of critical services. The Communication understood networks as

> "Systems on which data are stored, processed and through which they circulate. They are composed of transmission components (cables, wireless links, satellites, routers, gateways, switches etc) and support services (domain name system including the root servers, caller identification service, authentication services, etc.). Attached to networks is a n increasingly wide range of applications (e-mail delivery systems, browsers, etc.) and terminal equipment (telephone set, host computers, PCs, mobile phones, personal organisers, domestic appliances, industrial machines, etc.)."[72]

Its security features were identified in the three canons of computer security, plus a fourth:

- Availability: services are accessible and operational as expected;
- Confidentiality: unauthorized parties cannot intercept communications/ read stored data;
- Integrity: the data transmitted or stored are unchanged and complete;
- Authentication: the identity claimed by users or entities can be established. It has to include the possibility of anonymization.

Consequently, it defined network and information security as

> "the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions. Such events or actions could compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data as well as related services offered via these networks and systems."[73]

The Commission identified six groups of network security incidents, together with their consequences, possible solutions and related challenges:

1. Interception of communications, namely wiretapping of network lines, or the interception of radio transmissions (i.e. at the physical level), which may lead to data alteration (i.e. at the content level, requiring encryption of traffic – for operators – and of data – for users);
2. Unauthorized access to computers or computer networks (with the objective to copy, modify destroy the data), namely dictionary attacks, brute-force attacks, social engineering, and password interception, commonly referred to as hacking. Proposed solutions include password controls and firewalls (for users), as well as attack recognition, intrusion detection and application level controls (for operators);
3. Network disruption, namely the exploitation of the "weaknesses and vulnerabilities of network components (operating systems, routers, switches, name servers, etc.)."[74] Examples include: name servers attacks, leading to disruptions in emails delivery or making certain websites unreachable, which require DNS servers encryptions; routing attacks, whereby traffic can be maliciously redirected to a different destination than the one requested; flooding and denial of service attacks (hereafter DoS), whereby the access to a website is blocked by means of overloading the server hosting it with more requests than those that it can handle (similar to

[71] European Commission, COM (2001) 298 final, 6 June 2001, p. 3.

[72] Ibid., p. 9.

[73] Ibid., p. 3.

[74] Ibid., p. 12.

blocking fax machines with repeated, long messages), requiring basic filtering and hard security on terminal servers.

4. Malicious software that modifies or destroys data, namely viruses, worms, Trojan horses, logic bombs, which can be handled with antivirus software.
5. Malicious misrepresentation of people or entities, to induce users to communicate confidential information, downloading malicious software etc., now referred to as phishing, pharming and identity theft. Proposed solutions include VPN using Secure Socket Layer (SSL) and IPsec, and certification;
6. Environmental and unintentional events, such as natural disaster, third parties, human error and hardware or software failure, which could compromise the network. Solutions include redundancy and infrastructure protection, and third-party liability.

Moreover, the Communications recognized that the list was not carved in stone due to continuous technological developments, and that, while security was being commoditized, the market suffered from failures, which a European policy needed to address.

The Commission therefore proposed seven clusters of initiatives. First, undertaking public awareness raising campaigns, in order to address the market imperfection of asymmetric information. Secondly, creating a European warning and information system, based on stronger Computer Emergency Response Teams (hereafter CERTs) at the MS level,[75] and on improved co-ordination among them. CERTs were to collect and analyse data about existing and emerging security threats, as well as plan forward-looking responses. Thirdly, providing technology support, by funding R&D in security and promoting interoperable encryption. Fourthly, undertaking work on standardisation and certification of market solutions (electronic signatures, certificates etc.), to solve one of the causes of market under-provision of security. Fifthly, working with international organisations (i.e. OECD, G8, etc.), given the global nature of the network infrastructure. Sixthly, incorporating security solutions in MS' e-government and e-procurement activities, as well as introducing electronic signatures when offering public services. Finally, adopting the necessary legal framework, such as facilitating the acquisition of encryption and the adoption of cybercrime legislation; however, "the legitimate concerns about cyber-crime…should not create solutions where legal requirements lead to weakening the security of communication and information systems."[76] In regard to the necessary legislative framework, the Communication asserted that

> "the proposed policy measures with regard to network and information security have to be seen in the context of the existing telecommunications, data protection, and cyber-crime policies. A network and information security policy will provide the missing link in this policy framework."[77]

As in the previous Communication, the Commission recognised not only that "protection of privacy is a key policy objective in the European Union"[78], but also that the provisions contained in the Data Protection Directives contribute to the objectives of network security, and explicitly listed the abovementioned article 17 of Directive 95/46/EC and articles 4-5 of Directive 97/66/EC.

The Communication was subsequently endorsed by the Council.[79] Future initiatives have therefore developed according to the 'three-pronged approach,' as addressed in the next section.

---

[75] The very first CERT was created at Canergie Mellon to respond to the virus 'Morris worm' in the 1980s.

[76] European Commission, COM (2001) 298 final, 6 June 2001, p. 26.

[77] Ibid., p. 3.

[78] Ibid., p. 24.

[79] *Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security*, OJ C 43, 16.2.2002, p. 2.; Council Resolution, O JC 48, 28/02/2003, p. 1-2.

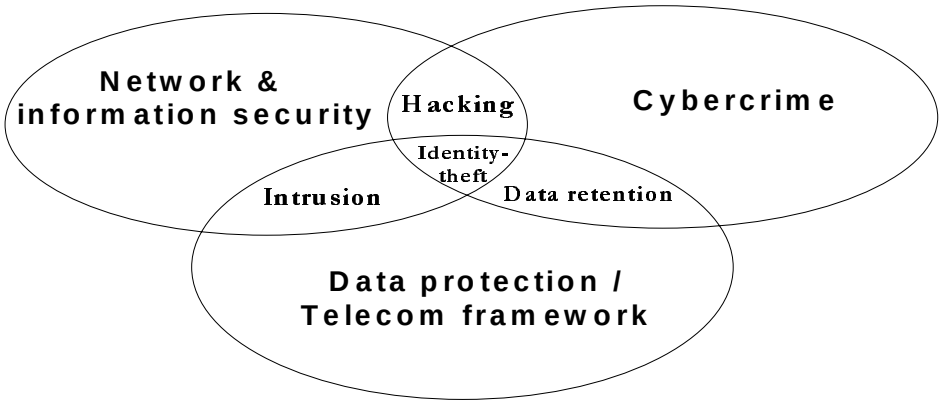

Figure 1. The Three-Pronged Approach, COM (2001) 298, p. 3

2.3 The Three-Pronged Approach

2.3.1 Initiatives in the area of telecommunications and privacy (former first pillar?)

The body of related legal instruments grew in the years following. In 2000, the Electronic Commerce Directive[80] was adopted to regulate Information Society Services (hereafter ISS), whereas Directive 2002/21/EC[81] addressed the provision of electronic communications. In article 1 of Directive 98/34/EC, as amended by Directive 98/48/EC,[82] ISS are explicitly excluded from the concept of a publicly available electronic communications service.[83] Such distinction is crucial, as the e-privacy Directive (article 3), which was reviewed in 2002, and the 2006 Data Retention Directive, do not apply to ISS.

The reviewed e-privacy Directive (2002/58/EC) introduced a number of innovations, which are relevant for this discussion. Article 6 provides that traffic data has to be made anonymous when it is no longer needed for the purposes of the transmission of a communication, and article 9 further specifies that location data other than traffic data may only be processed when made anonymous, exclusively for the duration necessary for the provision of value added services, and made conditional upon the consent of the user.

Unsolicited communications (article 13), which includes electronic mail, are allowed provided that: i) subscribers have given their consent; or ii) that users are given the opportunity, free of charge and in an easy manner, to object to the use of their electronic contact details; and iii) the sender is not disguised, or the address used is not valid. In practice, this clause prohibits spam.

The e-privacy Directive was amended by the Data Retention Directive, adopted in 2006 with a view to harmonise MSs' provisions on data retention, in order to make such data available for the purposes of investigation, detection and prosecution of serious crimes, which can be extended to cybercrime. "Data Retention falls in this section because, in the action for annulment lodged by Ireland, the Court

[80] Directive 2000/31/EC, OJ L 178/1, 17.7.2000. p. 1-16.

[81] Directive 2002/21/EC, OJ L 108/33, 24.3.2002, p. 33-50.

[82] Service is "any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" (amended article 1(a) 2, Directive 98/48/EC, OJ L 217, 5.8.1998, p. 18–26).

[83] Maria Grazia Porcedda, "Law Enforcement in the Clouds."

of Justice of the EU (hereafter the ECJ) has confirmed the first pillar nature of the Directive,[84] under the jurisprudence of the essential/ancillary objective[85].”[86]

Although a data retention regulation is needed for a proper EU cyber-security policy in the AFSJ, its adoption sparked much debate. Indeed, it is considered poorly conceived under a technical point of view,[87] it would not respect the necessity and proportionality principles that would keep it in line with privacy laws,[88] and it would finally allow room for manoeuvre that is at odds with its harmonizing purposes. In addition, due to the combination of the recent court cases concerning Data Retention and the fact that it is a pre-Lisbon piece of legislation, it may well be overhauled soon.

The e-privacy Directive was amended once more by the so-called ‘Telecom Package’[89] in 2009. The amended article 5(3) explicitly prohibits storing information, or gaining access to information already stored in the terminal equipment of a subscriber or user, unless the subscriber or user has consented to it, after having been given clear and comprehensive information. In practice, article 5(3) bans the use of cookies or third party cookies for behavioural advertising, and aims at implementing an opt-in, rather than an opt-out, system for such data.

The reviewed article 4 allows the relevant national authorities, notably Data Protection Authorities (hereafter DPAs), to audit the security measures undertaken. Moreover, and very importantly, it introduces a mandatory notification of data breaches to the competent national authorities, and to the subscriber “when the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual…without undue delay.” Such notification is not obligatory if the provider “has demonstrated…that it has implemented appropriate technological protection measures…to the data concerned by the security breach” provided they “render the data unintelligible to any person who is not authorised to access it,” notably by means of encryption. A personal data breach is defined as a “breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed” (article 2(h)).

The Communication ‘A Digital Agenda for Europe,’[90] which was adopted in 2010 to address the policy needs for a successful digital internal market, called, among others, to make full use of mandatory notification of data breaches. Yet, only providers of public electronic communications services in the Community are obliged to notify breaches,[91] which significantly undermines its beneficial effects, even if MSs can decide to extend the obligation at the national level (to the detriment of harmonization). Actually, recital 59 of the amending Directive reads “the interest of users in being notified is clearly not limited to the electronic communications sector, and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at Community level

---

[84] European Court of Justice. Case C-301/06: *Judgment of the Court (Grand Chamber) of 10 February 2009 — Ireland v. European Parliament, Council of the European Union*. OJ C 82, 4.4.2009, p. 2–3.

[85] The essential objective of the Directive is that of regulating the providers' retention of data, whereas data access by LEAs is only the ancillary object, because it is not addressed by the Directive itself. Els De Busser, Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters Between Judicial and Law Enforcement Authorities (Maklu Uitgevers N.V., 2009); Hielke Hijmans and Alfonso Scirocco “Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help?” Common Market Law Review 46 (2009): 1485-1525.

[86] Porcedda, “Law Enforcement in the Clouds,” p. 218.

[87] See the work of the Platform on Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime, at the page <http://ec.europa.eu/home-affairs/policies/police/police_data_experts_en.htm>.

[88] Article 29 Data Protection Working Party, WP 172.

[89] Directive 2009/136/EC of 25 November 2009, OJ L 337, 18.12.2009, p. 11–36.

[90] European Commission, COM (2010) 245 final, 19 May 2010.

[91] There has been a fierce political fight on this point. Rosa Barcelò, “EU: Revision of the ePrivacy Directive,” *Computer Law Review International* 5 (2009): 129-160.

as a matter of priority." Accordingly, the European Parliament expressed its will to extend the obligation to notify personal data breaches.[92] The European Network and Information Society Agency (hereafter ENISA) and the WP29, which cooperate on data breaches notification,[93] have recently released a report on the subject.[94]

The measure is crucial in that it creates legal and social (reputational) incentives to implement both security and privacy measures, incentives that are missing so far. The point has been addressed in the proposal for a Regulation[95] adopted pursuant to a new legal base for data protection in the Lisbon Treaty. The innovations introduced by the proposed Regulation go well beyond the notification of data breaches; the subject is addressed in chapter 0.

It is worth going briefly back the abovementioned Digital Agenda for Europe, because, fifteen years after the Bangemann report, the text is striking for raising the same questions which were, for instance, addressed in the COM(2000) 890, with the necessary updates in the light of the technological innovations, and in particular the advent of cloud computing (which I will discuss in chapter 0). While cybercrime – ranging from child abuse to identity theft and cyber-attacks – and proper enforcement of privacy and data protection were among the priorities, the same measures as 10 years before were proposed, which may suggest that little advancement has taken place ever since. Actually, one may say that the EU may have taken a step backwards.

In Spring 2011, the Commission adopted 'The open internet and net neutrality in Europe' Communication,[96] which addresses the problem as to whether the data should flow freely or be discriminated according to the content they carry, and in particular to manage traffic and charge for the use of services requiring considerable bandwidth. The problem is closely related to filtering, which I will discuss in section 2.4.1. The EDPS has dubbed the Commission's approach to the problem as 'wait and see.'[97]

2.3.2 Initiatives in the network and information security realm

Activities in the area of network and information security pertain to the Directorate General on Information Society, currently under the leadership of Commissioner Neelie Kroes. For the purposes of this discussion, it is important to highlight the creation of ENISA, as well as four Communications.

ENISA was established in 2004 with the objective of "ensuring a high and effective level of network and information security within the Community and in order to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the EU."[98] ENISA's mandate was renewed in 2008 and again in 2011, and its role was expanded to allow it to provide a wider support in network security.

Communication COM(2001) 298 on 'Network and Information Security' addressed the importance of communication networks for the provision of civil society services, for instance electricity, water, oil and gas. A typical example is that of Supervisory Control and Data Acquisition (hereafter SCADA)

---

[92] See at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//EN>.

[93] See at <http://www.enisa.europa.eu/media/news-items/closer-cooperation-between-the-agency-art.-29-data-protection-working-party>.

[94] ENISA, *Recommendations on Technical Implementation Guidelines of Article 4*, Crete, April 2012.

[95] European Commission, COM (2012) 11 final.

[96] European Commission, COM (2011) 222 final, 19 April 2011.

[97] EDPS, *Opinion on Net Neutrality, Traffic Management and the Protection of Privacy and Personal Data*, Brussels, 7 October 2011.

[98] Regulation 460/2004/EC, OJ L 077, 13/03/2004 pp. 1-11, article 1.

computing systems, which manage the provision of such resources. The concept of communication networks (which are crucial for the provision of civil society service) was better defined by the Commission's 2005 'Green Paper on a European Programme for Critical Infrastructure Protection.'[99]

Communications networks are critical information infrastructure (CII), namely

> "ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)."[100]

In turn, Critical Infrastructure (CI) was defined as

> "those physical resources, services, and information technology facilities, networks and infrastructure assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments." One of the three types of infrastructure assets is composed of "public, private and governmental infrastructure assets and interdependent cyber and physical networks."[101]

The framework established in 2001 was reviewed in 2006 by the Communication 'A strategy for secure information Society- dialogue, partnership and empowerment.'[102] While the three-pronged approach was kept, the text encouraged fostering a culture of security based on the following elements: an open and multi-stakeholder process; structured dialogue; partnerships leading to better awareness and better understanding of the challenges; and the empowerment of all stakeholders, aimed at increasing everybody's responsibility. The Communication highlighted the importance of openness and interoperability to enjoy technological diversity, and encouraged the European industry to prosper. The Communication envisaged, *inter alia*, building partnerships for data collection and alert systems, developing multi-stakeholder dialogues on trusted computing and Privacy Enhancing Technologies (hereafter PETs).[103]

The following year, awareness on cyber-security in Europe and worldwide was raised by the cyber-attacks[104] suffered by Estonia and Georgia. Estonia is one of the most 'wired' countries in the world, where e-banking, e-health, e-learning and e-taxing are common,[105] although in 2007 such dependence was not matched by corresponding IT security equipment. The most accredited version is that the attacks –distributed denial of service (hereafter DDoS)[106] attacks of the intensity of 95 Mbps– were sponsored by Russia, after a statue of Stalin was removed from a town. Yet, in the end, the connection has never been proved, and the only person convicted was a Russian Estonian. The case showed the problem of attribution in cyber-attacks, i.e. the fact that it is difficult to establish the identity of the perpetrator(s). The year after, Georgia was attacked (and it counter-attacked), too. The evidence in this

---

[99] European Commission, COM (2005) 576 final, 17 November 2005, p. 20.

[100] Ibid., p. 19.

[101] Ibid., p. 20.

[102] European Commission, COM (2006) 251, 31 May 2006.

[103] The strategy was subsequently endorsed by *Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe*, OJ C 068, 23.3.2007, p. 1-4.

[104] The first documented successful cyber-attack seems to have taken place during the cold war, and was directed against the 1982 Siberian gas pipeline. Peter Sommer and Ian Brown, *Reducing Systemic Cybersecurity Risks*, OECD/IFP Project on 'Future Global Shocks', (Paris: OECD, 14 January 2011).

[105] House of Lords. *Protecting Europe against large-scale cyber-attacks*. European Union Committee, 5th Report of Session 2009-10, 18 March 2010.

[106] A DDoS attack is a Denial of Service attack (DoS) perpetrated by means of a botnet, which is a group of many compromised machines (zombies), whose control has been achieved prior to the attack, usually via the use of Trojan-horse programs. DDoS combine the insecurities of endpoints with those of Internet protocols. Susan Landau, *Surveillance or Security? The Risks Posed by Wiretapping Technology* (The MIT Press, Cambridge: 2010). See also Sommer and Brown, *Reducing Systemic Cybersecurity Risks*, p. 24-25.

case leads to private actors. The events took place during the war with Russia and were of a bigger scale than Estonian attacks (800 Mbps).

The Communication 'Protecting Europe from Large Scale Cyber-attacks and Disruptions: Enhancing Preparedness, Security and Resilience'[107] recognised the relevance of this new form of threat and specifically addressed it, by proposing an action plan based on five pillars: prevention and preparedness, detection and response, migration and recovery, international cooperation, and the development of criteria for selecting European Critical Infrastructures in the field of ICT. It also suggested raising awareness and defining a plan of immediate actions to strengthen the security and resilience of CIIs. These activities were meant to complement actions in the AFSJ.

The Communication was endorsed by the Resolution 'on a Collaborative European Approach to Network and Information Security'[108] through which the Council claimed that "new usage patterns, such as cloud computing and software as a service, put additional emphasis on the importance of Network and Information Security" and declared that "there is a need to enhance and embed Network and Information Security in all policy areas and sectors of society, and to address the challenge of ensuring sufficient skills via both national and European actions and raising awareness among users of ICT."[109] The Council endorsed the expansion of the role of ENISA, as well as the increasing use of multi-stakeholder models such as PPPs; it recognised the vital role played by providers, the importance of national CERTs, whose activities were to be intensified, and of intra-EU and extra-EU cooperation. Finally, it recommended using the OECD Security Guidelines as a model for similar European guidelines. I will address this issue in depth in the next chapter. While the Resolution is not revolutionary as far as its content is concerned, it looks at cyber-security as being fundamental for all sectors of society. This is in line with the documents released in the cybercrime area, as well as in CFSP.

Finally, the Communication 'Achievements and Next Steps: Towards Global Cyber-security'[110] appraised the steps taken and updated the measures needed for each pillars established by the Communication 'Protecting Europe from Large-scale Cyber-attacks and Disruptions', in line with the Council Resolution above. On the topic of preparedness and prevention, it called for the European Forum of MSs to share information and best practices, the development of a European PPP for Resilience, and establishing the threshold for CERTs services and capabilities. As for detection and response, it proposed the development of a European Information sharing and Alert System for citizens and Small and Medium Enterprises (SMEs). As for migration and recovery, it proposed MS to develop national contingency plans, and the organization of national and European exercises. On the topic of the international and EU-wide cooperation, it called for the establishment of European principles and guidelines for the resilience and stability of the Internet. Finally, it reconfirmed the need to set criteria to identify CII in the ICT sector.

The text seems to reveal that little progress has been made in the past couple of years. Finally, it is worth noting that in June 2011, an EU CERT was created.[111]

---

[107] European Commission, COM (2009) 149 final, 30 March 2009.

[108] *Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security*, OJ C 321 of 29.12.2009, p. 1-4.

[109] Ibid. p. 2.

[110] European Commission, COM (2011) 163, 31 March 2011.

[111] The EU Security Roundtable, *European Cyber Security Conference Shared Threats – Shared Solutions.*

2.3.3 Initiatives in cybercrime

I shall now take a step back in time to address the initiatives taken in cybercrime. Two area-specific laws were adopted in the field: the Council Framework Decision 2001/413/JHA on Combating Fraud and Counterfeiting of Non-cash Means of Payment, and the Framework Decision 2004/68/JHA on Sexual Exploitation of Children,[112] which should reveal "the particular focus put by the Commission on the protection of children, especially in relation to the fight against all forms of child sexual abuse material illegally published using information systems, a horizontal priority which will be kept in the future."[113]

The first comprehensive result of the work undertaken in cyber-crime was the adoption of Council Framework Decision 2005/22/JHA,[114] the first law explicitly harmonising the criminalization of malicious conduct online. The Directive addressed a subset of offences included in the Cybercrime Convention, which was seen as a minimum threshold for standardization. Both the Convention and the Council Framework Decision are addressed in greater detail in chapter 0. For the moment, it is relevant to underline that, due to several shortcomings, the text is being repealed.

The Hague Programme further recognised the importance of cybercrime. The Action Plan implementing it[115] recommended improving European coordination and cooperation between high-tech crime units in MSs, and with the private sector (cybercrime intelligence network), including the development of a European cybercrime manual as a way of "strengthening prevention of organised crime."[116]

In 2007, the Commission published its follow-up to the 2000 Communication 'Promoting a Safer Internet',[117] which set out the main elements of a EU policy on cybercrime. First of all, it gave a working definition of cybercrime as "criminal acts committed using electronic communications networks and information systems or against such networks and systems," and clarified that it applied to three categories of criminal activities. These recall the categories contained in the Cybercrime Convention, as illustrated in the next chapter

> "The first covers traditional forms of crime such as fraud or forgery…The second concerns the publication of illegal content over electronic media (i.e. child sexual abuse material or incitement to racial hatred)…The third includes crimes unique to electronic networks, i.e. attacks against information systems, denial of service and hacking. These types of attacks can also be directed against the crucial critical infrastructures in Europe and affect existing rapid alert systems in many areas, with potentially disastrous consequences for the whole society. Common to each category of crime is that they may be committed on a mass-scale and with a great geographical distance between the criminal act and its effects. Consequently the technical aspects of applied investigative methods are often the same."[118]

The Communication recalled the three-pronged approach established in 2001, and the initiatives taken in other sectors, such as the provisions relating to network security contained in the e-privacy Directive. It then took stock of the development of cyber-crime, and called for: increasing LEAs

---

[112] Council Framework Decision 2001/413/JHA, OJ L 149, 2.6.2001, p. 1–4; Council Framework Decision 2004/68/JHA OJ L 013 20/01/2004 P. 0044 – 0048.

[113] European Commission, *Towards a general policy on the fight against cybercrime*, COM (2007) 267 final, 22 May 2007.

[114] Council Framework Decision 2005/222/JHA, OJ L 69, 16/03/2005, p. 67.

[115] *Council and Commission Action Plan implementing the Hague Programme on strengthening Freedom, Security and Justice in the European Union*. OJ C 198, 12.8.2005, p. 1-22.

[116] Ibid., p. 13

[117] European Commission, COM (2007) 267 final, 22 May 2007.

[118] Ibid. p. 2.

cooperation; the development of an appropriate policy framework; raising awareness on the problems of cybercrime; cooperating internationally; and developing PPPs. It highlighted the favourable nature of the latter in the fight against cyber-crime, as well as the need to encourage information sharing on crime. In general, the text strikes one as addressing the same issues as COM(2000) 890. Accordingly, the Presidency Conclusions of the Brussels European Council of 21/22 June 2007[119] urged the development of a policy within Justice and Home Affairs (AFSJ).

The cyber-attacks against Estonia and Georgia have certainly affected the attitude in cybercrime, too. In November 2008, Council Conclusions[120] called for the development of a comprehensive program against cybercrime, implying a joint working strategy between the MSs and the Commission, to combat crimes "as worrying as child pornography, any form of sexual violence and any act of terrorism," threats to the networks and "traditional forms of crime committed via the internet, such as identity fraud, identity theft, fraudulent sales, financial offences…"[121] In the short term, it urged improving PPPs, i.e. establishing points of contacts, fostering clear and prioritized cooperation request forms, and exchanging best practices; setting up a network of Heads of Police against cybercrime; and reinforcing technical and international cooperation with third countries. As for the short and medium term, the Council recommended, inter alia: establishing an EU reporting platform; working on the substantive legal aspects of cybercrime and the lack of statistics; and setting up joint investigation teams to assess the progress made.

At the same time, Europol was given a role in the fight against cybercrime, and was in particular designated as the point of convergence of the national alert platforms created by the G8 and endorsed by the Cybercrime Convention (Europol's European Cybercrime Platform, or ECCP). Shortly after, the Safer Internet Program 2009-2013 was adopted:[122] the objective being to fight illegal content online, as well as harmful conduct such as grooming and bullying, with particular reference to the web 2.0 (i.e. social networks).

Building on previously adopted documents, the 'Draft Council Conclusions on an Action Plan to Implement the Concerted Strategy to Combat Cybercrime' aimed at coping with cybercrime, intended as "child pornography, sexual violence, terrorist activities, attacks on electronic networks, fraud, identity theft, etc."[123] It also set out an action plan for the short, medium, and long term. The objectives for the short term included finding out more about perpetrators and their modus operandi, in order to have a better grasp of the phenomenon, developing filtering systems against child sexual abuse content and promoting the use of joint investigation teams. As for the medium term, the Council proposed a number of actions. Examples include training police, judges, prosecutors and forensic staff to carry out cybercrime investigations; encouraging information sharing between the MS' LEAs; gathering and updating best practices on technological investigation techniques and boosting the use of computer investigation tools by LEAs; promoting and boosting activities to prevent cybercrime, including the use of cyber-patrols; and setting up a documentation pool on cybercrime. The Council proposed establishing a centre with those functions within Europol.

---

[119] Council. *Presidency Conclusions, Brussels European Council 21/22 June 2007*. 11177/1/07, 20 July 2007.

[120] *Council Conclusions of 27 November 2008 on a concerted strategy and practical measures against cybercrime*. OJ C 62, 17.3.2009, p. 16-18.

[121] Ibid. p. 16-17.

[122] Available at: <http://ec.europa.eu/information_society/activities/sip/policy/programme/current_prog/index_en.htm>; *Council Decision No 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 Establishing a Multiannual Community Programme on Protecting Children Using the Internet and other Communication Technologies*. OJ L 348, 24.12.2008, p. 118-127.

[123] Council. *Draft Council conclusions on an Action Plan to implement the concerted strategy to combat cybercrime*. 5957/2/2010, Brussels, 25 March 2010.

These last two documents, as well as the Stockholm Programme, and the subsequent Internal Security Strategy and Action Plan to Counter Terrorism,[124] referred to cyber-security and cyber-crime as a growing threat, i.e. they tended to securitise it.

The Stockholm Programme[125] explicitly addressed cybercrime and, while it called for greater respect of privacy and data protection rules, there was no trace in the text of the three-pronged approach. Accordingly, the Action Plan of the Stockholm Programme suggested actions for cybercrime and Network and Information Security, first and foremost the promotion of the ratification of the Cybercrime Convention. It then advanced a new proposal on Attacks against Information Systems (indeed COM(2010) 149 which was analysed in the previous section) and it encouraged proposing a model of PPP on cybercrime issues by 2011. It set out the basis for the prolongation of ENISA's mandate, the adoption of rules on the protection of the network, and the creation of a EU cybercrime alert platform. It finally proposed to conduct a EU Security Survey by 2013, to collect statistics on cybercrime, and to adopt rules on the jurisdiction of cyberspace.

The Stockholm Program foresaw the adoption of an Internal Security Strategy. In the Draft Internal Security Strategy, cybercrime was portrayed as one the "main crime-related risks and threats which Europe faces today."[126] Relevant proposals were advanced by the actual Communication on the Internal Security Strategy, [127] according to which "the EU is exposed to an array of potential crises and disasters, such as those associated with climate change and those caused by terrorist and cyber-attacks on critical infrastructure […]."[128]

To tackle the 'growing threat' of cybercrime, the Communication proposed three actions at the EU level. Firstly, it recommended the creation of a cyber-crime centre, bound to become the main point to address cybercrime, in cooperation with the ENISA and the national CERTs. Secondly, it suggested to simplify the notification of cybercrime incidents by people, and to raise their awareness, to work with the industry to empower and protect citizens and to engage with international partners to strengthen the global risk management of IT networks. It announced the development of guidelines on cooperation to handle illegal Internet content– including incitement to terrorism– by 2011, and the creation of a platform to foster cooperation called 'Contact Initiative against Cybercrime for Industry and Law Enforcement.' Thirdly, in order to increase capabilities for dealing with cyber-attacks, it urged MSs to develop a CERT by 2012, which, in cooperation with the Commission and the ENISA, should also converge on a European Information Sharing and Alert System (EISAS), and implement response plans and exercises.

The EU 2010 'Action Plan on Combating Terrorism,'[129] a follow-up to the EU Counter-terrorism Policy,[130] addressed cyber-security in the context of terrorism. It referred to Stuxnet as an example of physical damage caused by a cyber-attack. Stuxnet[131] is the famous virus that allegedly delayed by two years the Iranian nuclear program. Stuxnet seems to have originated from a "hard-coded default password" [132] in the Siemens SCADA system, which reportedly used Internet protocols, sometimes over the public Internet. The episode has interesting implications for the debate on the interpretation of

---

[124] Council. *EU Action Plan on Combating Terrorism*. 15893/10, Brussels, 15 November 2010.

[125] *The Stockholm Programme*.

[126] Ibid. p. 2.

[127] European Commission, COM (2010) 673 final, 22 November 2010.

[128] Ibid. p. 14.

[129] Council, *EU Action Plan on Combating Terrorism*.

[130] European Commission, COM (2010) 386, 20 July 2010.

[131] For more information on SCADA and the Stuxnet, see at: <http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis> and <http://threatpost.com/en_us/blogs/dhs-thinks-some-scada-problems-are-too-big-call-bug-092611>.

[132] Sommer and Brown, *Reducing Systemic Cybersecurity Risks*.

articles 2.4 and 51 of the Charter of the United Nations, and in particular their application to cyber-attacks.[133] A more direct use of force, in fact, may have triggered the application of the provisions of the Charter. The Action Plan, then, stated that "work on Computer Network Operations, with an active contribution of the EU Military Committee, supports antiterrorism efforts in the domain of Cyber Space."[134] As a result, it reported the EU's participation in the US Cyber-storm exercise III and, in November 2010, the carrying out of 'Cyber Europe 2010,' the first exercise to test European (EU and EFTA countries) preparedness against cyber-attacks.

Finally, COM(2010) 157 laid down a proposal for a Directive on Attacks against Information Systems repealing Council Framework Decision 2005/222/JHA. The explanatory memorandum refers to the three-pronged approach, but the Preamble establishes a clear link with the Cybercrime Convention, whose provisions are in contradiction with the three-pronged approach. I address the proposed Directive in section 3.3.2.

2.3.4 Beyond the three-pronged approach: the Common Foreign and Security Policy & European Security and Defence Policy

The initiatives highlighted so far relate to the former first and third pillars only. It was only with the 2008 External Security Strategy[135] that the problem was addressed in CFSP. This is not surprising, given the EU institutional development. The External Security Strategy recognised that

> "modern economies are heavily reliant on critical infrastructure including transport, communication and power supplies, but also the internet. The 'EU Strategy for a Secure Information Society,' adopted in 2006, addresses internet-based crime. However, attacks against private or government IT systems in EU MS have given this a new dimension, as a potential new economic, political and military weapon."[136]

Thus, the Council called for more work in this area. The document marked a change in approach, in line with what happened in the previous two areas.

The European Defence Agency has also started tackling the issue, on top of what hinted at in the Action Plan on Combating Terrorism. The 2009 European Defence Agency capability development plan recognised that the cyber environment is a potential source of threat (cyber-warfare, cyber-attacks, but also a source for retrieving information) and set 2025 as a deadline to develop capabilities. The European Defence Agency refers to cyber-security as one "of the areas where it is natural to search for common approaches," which includes "maritime surveillance, intelligence, situation awareness, communications and information systems, cyber-security, maintenance, education and training & exercise."[137] It has called for making full use of the available tools, such as the European Framework Cooperation (EFC), an umbrella initiative, within which 'Situational Awareness' will be further investigated together with the European Commission and the European Space Agency, notably regarding issues from data collection to data sharing and dissemination, including aspects related to sensors, cyber security and information management."[138]

---

[133] Matthew C. Waxman, "Cyber-attacks and the Use of Force - Back to the Future of Article 2(4)," *Columbia Law School Working Paper*, September 2010. See also Lucas Lixinski, **"**Legal Implications of the Privatization of Cyber warfare," Academy of European Law, EUI Working Paper, Priv-war Project, AEL 2010/02, 2010.

[134] European Commission, COM (2010) 386, 20 July 2010, p. 35.

[135] European Council, *Report on the Implementation of the European Security Strategy– Providing Security in a Changing World (European Security Strategy)*. Brussels, S407/08, 10 December 2008.

[136] Ibid., p. 7.

[137] European Defence Agency. Bridging Efforts (Conference). Connecting Civilian Security and Military Capability Development. Bulletin 14, May 2010, p. 10.

[138] Ibid., p. 36.

In CFSP and CSDP, the focus is on the possibility of cyber-warfare. Yet, there are serious opponents to this possibility, as I will address in the section below.

2.4 The Policy Framework (and Cyber Landscape) in Synthesis

The reconstruction of the cyber-security policy provided here is only partial. The Resolutions of the Parliament, for instance, as well as other documents relating to specific initiatives, have been omitted for the sake of succinctness. Yet, the documents allow the isolation of a number of characteristics of cybercrimes and of the environment where they interact with cyber-security and data protection. Those characteristics are essential for policymaking in the area.

- Reliable statistics are still missing, since cybercrime is one of the most underreported crimes,[139] due to several overlapping causes.
- To begin with, the average user may lack awareness of the fact that what s/he faces is a crime. Indeed, raising awareness is one of the recurring proposals of the policy documents.
- Secondly, businesses do not always report incidents and breaches, because they fear reputational loss, and are often not legally obliged to report breaches. Truly, if the issue is finally rendered public, the delay in releasing the piece of news can act as a boomerang, yet the power of the media to generate shame works as long as the subject creates sensation, and loses clout when there is an overproduction of similar stories.
- Thirdly, the police lack the necessary tools, such as a database on reported and prosecuted cybercrimes. In the UK, for instance, the Home Office itself does not keep a database of 'e-crimes'.[140] As a result, there is no possibility of tracing back the use of the Internet in committing the crime. In addition, when a crime is reported to the police, it often looks like a minor offence. But what appears to be a €100 scam, which is not worth the time and money for an investigation, can in fact be a fraud costing millions, set up by organised crime, distributed around the world, which would definitely deserve resources for an investigation.[141] An exception to the rule is being established in the US, by far the most advanced country in combating cybercrime,[142] where the FBI has created the Internet Crime Complaint Center website. Individually minor crimes are compared and aggregated to understand the links that may pave the way to federal investigations. Identity theft crimes are also reported to the police first, and then investigated by the Federal Trade Commission (FTC).[143] Several proposals highlight the need to build a common reporting tool.
- LEAs remain inappropriately trained to tackle cyber-crime; indeed, it seems that, so far, LEAs only focus on those crimes that are likely to end up in successful investigations.[144] This, in turn, undermines the efficacy of the punishment, thus raising the incentives for offenders.[145] Many recent proposals try to address this lack of training.
- Another need, that of common definitions, may also contribute to the problem of underreporting, since the same phenomena may be defined differently in diverse countries, thus hindering comparison, when such data are available. The definition of cyber-crime is still very broad, and

---

[139] Kshetri, *The Global Cybercrime Industry*.

[140] In addition, customers must report online frauds to the association of bankers, which will decide in turn whether to notify the problem to the authority. The system is cumbersome, and it is not surprising that frauds are under-reported.

[141] House of Lords, *Personal Internet Security*.

[142] House of Lords. *Protecting Europe against large-scale cyber-attacks*.

[143] House of Lords, *Personal Internet Security*.

[144] Sommer and Brown, *Reducing Systemic Cybersecurity Risks*.

[145] Nir Kshetri, "Information and Communication Technologies, Strategic Asymmetry and National Security," *Journal of International Management*, 11 n° 4 (2005).

encompasses both traditional crimes and proper cybercrimes. I will address this in detail in section 2.4.

- PPPs are still at the core of the measures proposed. While their importance is indisputable, it is difficult to describe how they work in practice.[146] These partnerships are not always easy, either because LEAs' requests can be onerous for businesses or difficult to address, or because of the procedures that must be respected by companies, as well as the intrinsic volatility of the data. Also, companies may fear that the government will not keep their industrial secrets or that cooperation may lead to monitoring of their communications, with consequential loss of trust by consumers.[147] Indeed, co-operation tends to take place in an informal, i.e. unregulated, setting. So far, stringent measures on these partnerships do not exist, as shown by the most recent policy documents.
- Another proposed measure, content filtering, is still on the agenda today, and is at the centre of a strong debate, as I will address in section 2.4.
- The Cybercrime Convention is the legal instrument of reference. I will address the benefits of such a choice in chapter 3.
- Early Communications from the Commission acknowledged the insufficient provision of security by the market. The problem is still relevant, and is well known at the technical level.[148] In fact, software companies enjoy a first mover advantage when they release new products; since testing is a long procedure, they prefer launching an imperfect program on the market, and then compensate for security flaws with patches and updates. Many viruses, though, exploit these errors in the systems, so they probe programs constantly for flaws. This rash of flaws and patches has been dubbed the 'arms race.'[149] Since the error rate increases with the size of the program (measured in SLC or Source Lines of Code), and as SLC has increased dramatically, security fallacies have progressively increased.[150] In brief, the incentives of businesses and individuals for security are misaligned, since those who bear the losses deriving from a security failure – the individuals – are not the same who should invest in security – the businesses. As a result, there is rational under-spending in security.[151] This is not always clear in the new policy documents.
- Technology is evolving, the new frontier now being cloud computing, which I will address extensively in section 4.4, and big data.[152] Here, it is useful to underline that, while cloud computing solves some of the security threats and vulnerabilities relating to storing data on one's PC (i.e. keeping one's programme updated, or avoiding viruses), the concentration of data makes them more attractive to cyber criminals.
- Large-scale cyber-attacks can have a strong impact, and must be tackled accordingly. Some predict a cyber-war scenario. Cyber-war, though, is unlikely due to the problem of attribution (either of machine, human or digital identity[153]), and the ensuing need of keeping the attacks short and limited. In fact, the longer the attack, the higher the chance for the victim to buffer the offence, and to identify the attackers. In other words, it is difficult to respond to an attack, unless it is long enough. Consequently, attacks tend to be short and circumscribed, which in turn limits the chances of reprisals and, as a result, the role of the military. Blended attacks, i.e. an attack (to

---

[146] House of Lords, *Protecting Europe against large-scale cyber-attacks*.

[147] Ibid.

[148] Landau, *Surveillance or Security?*

[149] House of Lords, *Personal Internet Security*.

[150] Giovanni Sartor, *L'Informatica Giuridica e le Tecnologie dell'informazione* (Torino: Giappichelli, 2010).

[151] Sommer and Brown, *Reducing Systemic Cyber-security Risks*.

[152] Lohr, Steve, "The Age of Big Data" *New York Times*, 18 February 2012.

[153] Landau, *Surveillance or Security?*

networks) perpetrated together with a conventional kinetic attack to disorient the victims, may be more likely than a proper cyber-war.[154] Nevertheless, a cyber-security industrial complex seems to be emerging.

- The forensic techniques required to investigate different crimes are the same in the online environment.
- There is a growing call for cross-border and international cooperation and information exchange.
- Despite a clear vision of what are the challenges and needs in the area, there does not seem to be an organic policy plan. The situation might change by the end of 2012.[155]

The second element emerging from this brief reconstruction, and in particular the 'three-pronged approach', is that privacy and data protection, network and information security and tackling cybercrime are seen as different aspects of the same phenomenon (ensuring a safe development of the information society), which complement one another. In principle, therefore, the second hypothesis is supported: the policy documents not only acknowledge that privacy and data protection are not at odds with cyber-security and cybercrime prevention; some of the provisions contained in the EU privacy/data protection regime can even play an important role in the prevention of certain types of cybercrimes, and in particular network and information security and cybercrime 'proper'.

Nevertheless, when the Commission deals with cybercrime, it does so from the point of view of prosecution, where privacy and data protection have little role to play, apart from the rights of potential suspects or individuals affected by the investigation. This may well be due to the importance attributed to traditional crimes committed by electronic means, where reactive and forensic measures play a greater role (at the same time, though, the Commission seems to recognize that the forensic techniques are the same for both traditional and new crimes, which supports a portion of the first hypothesis I made).

In addition, since Estonia has suffered the cyber-attacks, the Commission and the Council seem to have changed their approach towards cyber-attacks, and cybercrimes in general, which are presented as existential threats to the nation and the Union. In other words, the issue seems to have been securitized.[156] Radical measures and information sharing, rather than prevention, are being proposed. Finally, as far as the most arduous issues are concerned, and in particular filtering, the Commission seem to have adopted a wait-and-see approach.

This combination puts at risk the possibility of a *de iure* integration. The next chapter addresses the legal framework in greater detail, and tries to explain why law should follow what is a *de facto* integration.

[154] Ibid.

[155] Nikolaj Nielsen, "EU cyber-security legislation on the horizon," *Euobserver.com*, 11 May 2012.

[156] Barry Buzan et al., *Security: a New Framework for Analysis* (Boulder, CO: Lynne Rienner 1998).

3. Cybercrime and Cyber-Security: First Hypothesis and One Caveat

3.1 Introduction

As follows from the previous section, there are relatively few cybercrime and cyber-security legal instruments applicable in the EU, namely:

- International legal instruments:
    - Binding Treaties and Conventions: the CoE Cybercrime Convention, the only international instrument adopted hitherto (to which the EU is not a signatory);
    - Non-binding instruments and soft law: UN, CoE and EU Recommendations, and OECD Guidelines;
- Laws in the former third pillar:
    - Comprehensive instruments: Council Framework Decision on Attacks against Information Systems 2005/222/JHA, and the proposal repealing it;
    - Sectoral laws: Council Framework Decisions on banking, child pornography and intellectual property.

The entry into force of the Lisbon Treaty has eliminated the pillars structure of the EU and has 'communitarised' the third pillar, whose legal instruments will now be adopted according to the ordinary legislative procedure. Indeed, the instrument repealing Decision 2005/222/JHA will be a Directive, in accordance with its new legal base, article 83(1) TFEU.

Regardless of the institutional changes, the 'Communication on a proposal for a Directive on attacks against information systems repealing Council Framework Decision 2005/222/JHA' builds on the policy framework set up so far – not only on the three-pronged approach, but also on the Cybercrime Convention. As put by recital 8 of the proposal, "the Council Conclusions on 27-28 November 2008 indicated that a new strategy should be developed with the MS and the Commission taking into account the content of the 2001 CoE Cybercrime Convention. That Convention is the legal framework of reference for combating cybercrime, including attacks against information systems. This directive builds on that Convention." Before continuing the analysis of the proposal, it is therefore necessary to review the two instruments on which it rests, i.e. both the Decision to be repealed, and the Cybercrime Convention, to which I turn my attention now.

3.2 The CoE Cybercrime Convention

The Cybercrime Convention was submitted to the Committee of Ministers and opened for signature in Budapest, on September 23, 2001.[157] Work on it began in 1996 with the objective of reaching a more comprehensive legal instrument on cybercrime than Recommendation No 89 (9). The negotiations were undertaken by the *ad hoc* Committee of Experts on Crime in Cyber-space (PC-CY); four non-CoE states took part in the drafting, namely United States, Canada, Australia and South Africa.

In spite of recognising that "technical measures to protect computer systems need to be implemented concomitantly with legal measures to prevent and deter criminal behaviour,"[158] the Convention[159] does

[157] For the updated list of countries having ratified the Cybercrime Convention, see <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>.

[158] Cybercrime Convention, *Explanatory Memorandum*, p. 2.

[159] In this section, I refer to the Cybercrime Convention simply as the Convention.

not address any such preventive measure. Rather, it addresses the problem by choosing criminalisation as a deterrent. As explained in the Preamble, it aims at establishing a common criminal policy, based *inter alia* on legislation and international co-operation (recital 4), as well as on cooperation between States and private industry – while protecting the legitimate interests in using and developing information technologies (recital 7) – mindful of the need to balance law enforcement with the respect of human rights enshrined in existing international agreements.[160] Consequently, the objective of the Convention is three-fold (recital 9): firstly, deterring (a) actions against the confidentiality, integrity and availability of computer systems, networks and computer data and (b) the misuse of such systems/network data; secondly, adopting sufficient powers, domestically and internationally, to combat, detect, investigate and prosecute, such criminal offences; and thirdly, providing arrangements for fast and reliable international co-operation. Accordingly, the text is divided into four Chapters: (i) use of terms; (ii) measures to be taken at the domestic level – substantive law and procedural law; (iii) international cooperation; and (iv) final clauses.

The Convention is undoubtedly a valuable instrument, since several countries lacked specific legislation on procedural aspects of cybercrime, which is compelling due to the volatility and vulnerability of electronic evidence (i.e. it can quickly disappear and be easily compromised). Indeed, the lack of common rules can impede international cooperation– which is fundamental, given that evidence is often dispersed – as shown for instance by the 'Love letter' virus investigations. In that instance, the US could not prosecute the Filipino hackers who authored the virus, since their deed was not a crime in the Philippines when it was committed.[161] The lack of common rules can also foster the proliferation of 'digital crimes havens'.[162] Accordingly, states that are not members of the CoE, in Latin America and in the Middle East, are using the Convention as a model framework.[163]

Yet, the opposition to the Convention of two global powers such as China and Russia 'over concerns that police might acquire powers across national boundaries without consent from the local authorities,'[164] deeply undermines its efficacy. Indeed, to work properly, the Convention should be globally endorsed.[165] The adoption of a more comprehensive international legal instrument on cyber-security and cybercrime, though, may have so far been hindered by two factors: the convenience of 'cyber weapons' for certain countries, since cyber-capabilities can reduce the asymmetric differences in power between countries;[166] and the different ideological and cultural contexts, which affect technical preferences.[167] In this respect, the Convention may represent the maximum agreement achievable between such diverse countries,[168] and as such a necessary evil. Recently China, Russia, Tajikistan and Uzbekistan proposed in a letter to the UN Secretary General[169] an international code of

---

[160] These include, *inter alia*, the ECHR, the United Nations Covenant on Civil and Political Rights, the CoE Convention 108 on the Protection of Personal Data, the UN Convention on the Rights of the Child and the ILO Worst forms of Child Labour Convention.

[161] Fawzia Cassim, "Formulating Specialised Legislation to Address the Growing Specter of Cybercrime: a Comparative Study." *Potchefstroom Electronic Law Journal 12, n° 4 (2009)*; Kshetri, "Information and Communication Technologies"; Maria Grazia Porcedda, *Transatlantic approaches to Cyber-security.*

[162] Victoria Nash and Malcolm Peltu, "Rethinking Safety and Security in a Networked World: Reducing harm by Increasing Cooperation", Oxford Internet Institute, Forum Discussion Paper N° 6, November 2005.

[163] Sommer and Brown, *Reducing Systemic Cybersecurity Risks*.

[164] Ibid., p. 71.

[165] Brenner, *The Council of Europe's Convention on Cybercrime*.

[166] Waxman, "Cyber-attacks and the Use of Force."

[167] Busch in Nash and Peltu, "Rethinking Safety and Security in a Networked World."

[168] Clough, *Principles of Cybercrime.*

[169] United Nations. *Letter to the United Nations addressed to the Secretary General,* General Assembly. A/66/359, 14 September 2011.

conduct for information security, which may open a new international approach to the matter."[170] This is not the only defect of the Convention. Indeed, the doctrine has criticised the Convention in various manners, as I illustrate below.

3.2.1 Procedural law

The aim of the procedural section is to supplement existing mutual legal assistance treaties, or to substitute them in their absence, to address the problem of evidence preservation, location and sharing, as well as to determine which state has jurisdiction over a particular case. The innovations to the national procedural laws required to tackle the specificities of cybercrime (Chapter 1, Section 2), as well as the means of international cooperation (chapter 3), are at the heart of the Convention. Proposed measures include: obtaining and collecting all data[171] relating to subscribers, traffic[172] and content, whether in transit or stored, both by means of traditional methods such as search and seizure (or access and copying, in technological language), real-time collection of traffic data[173] and interception of content data,[174] subject to safeguards.[175] Other measures, such as the expedited preservation of data,[176] are introduced to remedy the volatility typical of data in an online environment.

In order to deal with requests for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence, and in particular to fulfil the need for immediate assistance to a requesting party, article 25 invites parties to establish a point of contact available 24 hours a day, 7 days a week, in line with the initiatives undertaken by the G8. The explanatory memorandum clarifies that the Convention does not allow a blanket collection of data for so-called fishing expeditions, nor does it oblige providers to assist beyond the means they possess. Yet, there are a number of problems.

First of all, the scope of procedural laws goes considerably beyond the list of offences found in the substantive law section (which is analysed in sub-section 2.2.2). Pursuant to article 14(2), the procedural measures apply to any offences committed by means of a computer system and the collection of evidence of a criminal offence in electronic form, both nationally and internationally. The Explanatory Memorandum offers a two-pronged rationale: on the one hand, states should enact laws providing for the use of information in electronic or digital format for evidentiary purposes. On the

---

[170] Porcedda, *Transatlantic Approaches to Cyber-Security*, pp. 43-44.

[171] The concept is based on the ISO definition: a representation of facts/information/concepts suitable for electronic processing by a computer system/program. Data may be both the object of an attack or of the application of investigative measures.

[172] Traffic data is any computer data related to or generated by a communication (therefore, auxiliary to it) via a computer system, which indicates the origin and destination (telephone number, IP address, or other identifier), route, time (GMT), date, size, duration and type of service (file transfer, instant messaging etc.), relating to a particular communication. Traffic data can provide information to collect further evidence; yet, it tends to be volatile and therefore needs to be somehow retained. The Convention allows states to grant different protection to these data according to their sensitivity, the minimum protection being provided for in article 15.

[173] It refers to the recording of traffic data at the time of communication.

[174] Regulated by article 21, it refers to anything transmitted over the network. The drafters deemed it crucial to determine whether the communication is of illegal nature, and to collect evidence of past and future crimes.

[175] In line with the ECHR jurisprudence, these include judicial independent supervision; specificity as to the communications or persons to be intercepted; necessity, subsidiarity and proportionality; limitation of the duration of the collection; and right of redress. Due to the privacy concerns raised by real time collection and, in particular, interception of content data, States can reserve the right to apply both articles 20 and 21 to serious offences only.

[176] This refers to keeping safe the data already retained, and is different from the retention of data, which means storing data. The retention and expedited preservation are subject to two different orders. Yet, Article 17 (expedited preservation and partial disclosure of traffic data) provides that it has to be made possible to ensure the rapid disclosure of the sufficient amount of traffic data to identify all service providers involved and the path followed by the data.

other hand, though, the existence of other types of computer crime than the ones listed by the Convention is acknowledged, thus implicitly stating the limited character of the Convention's provisions. The question is that article 14 seems to make the substantive provisions irrelevant.[177] It also paves the way to the concern voiced by the WP29, namely the widespread purpose creep of intrusive procedural and evidentiary measures. One of the three general principles on international cooperation (article 23) is exactly extending co-operation beyond the offences listed by the Convention, to the investigation or proceedings concerning, and the collection of evidence pertaining to, computer-related crime.

Secondly, although it is possible to make co-operation conditional upon the existence of dual criminality, the application of the latter is limited, so that assistance may be due by the requested party to the requesting party, for an act that is not considered an offence in the former.[178] According to article 25, co-operation should be the widest possible for both investigations and proceedings concerning offences relating to computer systems and data, and for the collection of evidence in electronic form of a criminal offence. Dual criminality is defined by article 25(5), in such a way as to avoid that parties apply too rigid a test. If a party requires dual criminality in order to grant assistance – i.e. sharing information –the crime does not have to be called or classified in the same way in the two countries; what matters is that the crime investigated has the nature of a criminal offence.

Article 27(3) on mutual assistance requests procedures provides that the technical procedural requirements applying in the mutual assistance requests should be those of the requesting party, unless these are against the legal principles of the requested party. The rationale is that the requesting party should be able to admit the evidence in court. The paragraph does not deal with fundamental procedural protections. Yet, the grounds for refusal by one party shall never be too heavy, so as to fulfil the overriding principle of the Convention, which is to make the assistance as wide as possible. For instance, refusal of assistance on data protection grounds may be invoked only in exceptional cases;[179] the parties should rather try to place conditions allowing the transfer of information. This article may be read as a way to formalize assistance, and avoid the creation of 'informal procedures'. Yet, this is somehow contradicted by article 32, whereby a party can unilaterally access computer data without seeking the authorisation of another party, when it is (a) publicly available stored computer data, regardless of its geographical location or (b) when it accesses or receives stored computer data located in another party, if it obtains the voluntary consent of the custodian of the data, which has the authority to lawfully disclose it, and such disclosure happens through a computer system located in the requesting party. This provision envisages the creation of 'informal situations,' especially since its wording is particularly vague (which was justified by the drafters due to a lack of concrete experiences to refer to).

Thirdly, safeguards and provisions pertaining to international cooperation procedures can be subject to reservations. Consequently, states applying higher safeguards[180] may not refuse cooperation on grounds of lower safeguards provided for by requesting parties. In many cases, this would mean transferring data "even when such transfer does not pass the test of necessity, proportionality and appropriateness typical of human rights."[181] For instance, while article 28 on confidentiality and limitation on use allows the requested party to: (a) impose to grant its assistance only if confidentiality is kept; (b) explicitly invoke that the content of the assistance is not used for investigations or

---

[177] Brenner, "The Council of Europe's Convention on Cybercrime."

[178] Ibid.

[179] Cybercrime Convention, *Explanatory Memorandum*, p. 48.

[180] Article 27 bis and 27(6), for instance, allows for the possibility (may instead of shall) to impose conditions as regards the confidentiality- not the protection of personal data- of the transfer, which is further limited by the caveat of public proceedings.

[181] Article 29 Data Protection Working Party, *Opinion 4/2001 On the Council of Europe's Draft Convention on Cybercrime, (WP 41)*, March 2001, p. 5; Porcedda, *Transatlantic Approaches to Cyber-Security*.

proceedings other than the one for which assistance was granted; there is a twofold, implicit, limit to the request of conditionality. Firstly, the requesting party may need to use the evidence obtained through the assistance in a public trial, which therefore renders the information public domain; secondly, in case the information is evidence exculpatory to an accused person, it must be disclosed to the defence or judicial authority, in line with the fundamental legal principles of many states.

This leads to the fourth and last point, i.e. the position of human rights, and specifically privacy and data protection, in the Convention. Article 15 lays down the mandatory conditions and safeguards to be applied when implementing the procedural provisions of the Convention. Pursuant to paragraph 1, State parties should respect the existing constitutional, legislative or judicial safeguards and each country's national and international conditions, including those enshrined in both the ECHR (and its jurisprudence, as well as the CoE's laws for its MSs) and the 1966 UN Covenant on Civil and Political Rights.[182] As for common standards and minimum safeguards, paragraph 2 lists: judicial or otherwise independent supervision; grounds to justify the application of the measures; limitation of the scope and duration of the powers and procedures employed. The determination of the precise content of these provisions is left to the States, together with the right of self-incrimination, legal privileges and the specificity of individuals and places. In addition (paragraph 3), states must consider the impact of said powers and procedures upon the rights, responsibilities and legitimate interests of third parties (that is, the service providers),[183] to the extent this is consistent with the public interests, such as minimising the disruption of consumer services, protection from liability for disclosure or measures facilitating the disclosure, and the protection of proprietary interests. As put by the Explanatory Memorandum, article 15 adds "certain elements as conditions and safeguards that balance the requirements of law enforcement with the protection of human rights and liberties."[184]

The clause has been criticised by the WP29, as privacy and data protection are not adequately protected in the Convention, whose confusing and vague wording contrasts with the CoE's long-standing tradition of respect of human rights. Article 15 suggests that human rights shall be protected only when it is due, and only to an *adequate* extent. The text of the Convention refers several times to the expression "law and other measures," also when addressing conditions and safeguards; yet, in order to limit human rights, appropriate instruments (i.e. laws) have to be enacted. The Cybercrime Convention does not enjoin State parties that are not members of the CoE to introduce safeguards and conditions to which CoE MSs are bound by means of its several treaties, such as the ECHR. For instance, while reference to Convention 108 on data protection was inserted in the Preamble, signing it was not made mandatory for state parties that are not members of the CoE. There could therefore be a clash for the EU MSs, which are bound to Convention 108 and Directive 95/46/EC (sometimes extended to the third pillar), between said laws and the text of the Convention. For instance, the provisions on traffic data do not allow a refusal of co-operation on the basis of data protection. Signatories that are not members of the CoE enjoy the benefits of the free co-operation allowed by the Convention, without committing themselves to enforcing strict conditions and safeguards to the human rights affected, once the data have been received.[185]

Human rights advocacy groups such as EPIC and Privacy International have argued that the US' participation to the drafting may have indeed allowed the watering down of guarantees to human rights, and in particular privacy and data protection (but not freedom of expression, which in fact forms part of an additional protocol), to take place, as well as the surreptitiousness of the works.[186]

---

[182] United Nations, International Covenant on Civil and Political Rights, New York, 16 December 1966.

[183] A service provider is an entity, in a broad sense, allowing users to communicate via a computer system or that processes or stores computer data on behalf of the aforementioned provider or user.

[184] Id.

[185] Article 29 Data Protection Working Party, WP 41.

[186] Access to the travaux préparatoires has not been granted to me by the CoE to date.

Indeed, the text was rendered public only at its 19th draft, thus excluding *de facto* the contributions of other stakeholders. As a result, the Convention was perceived as a text for LEAs by LEAs,[187] allowing the exchange of information between LEAs for purposes not strictly relating to cybercrime, as results for instance from the combination of articles 18(1) and 19(4).[188] In accordance with article 18, which lays down rules on the production order needed to obtain the disclosure of the preserved data, the person in possession or control of the stored data should submit that data, or information relating to a specific subscriber/customer in their possession or control. While the provision does not authorize parties to compel ISPs to provide information about groups of providers for data mining purposes,[189] article 19 allows State parties to the Convention to empower the competent authorities to compel any person (i.e. the system administrator) informed about the functioning of a computer system, or the measures applied to protect the data therein, to enable the undertaking of search and seizure.

3.2.2 Substantive law

Mindful of the comments made above, I shall now analyse the substantive law provisions laid down in chapter II of the Convention. The chapter aims at providing minimum standards and consensus in a technology neutral language for harmonisation purposes. All offences must: be significant, i.e. not petty; done 'without right', in that the same act may be legal if done 'with right'; and done 'intentionally', albeit the threshold for intentionality must be set by means of national laws. The latter can go further, or require additional caveats before criminalisation applies. The provisions are divided into four groups, each corresponding to a dedicated title.

Title one deals with 'the core' of computer related offences, i.e. offences against the confidentiality, integrity and availability of computer data and systems.

Article 2 criminalises illegal access, by any means, by individuals or organisations, to a part or whole of a computer system (if a system is public, there is no absence of right). This can be simply hacking, cracking or computer trespass, and can result in impediments, alteration, destruction, breach of information confidentiality or other secrecy, thus leading to other forms of criminal action. A computer system, pursuant to article 1 (a), encompasses any device (hardware or software) or group of interconnected devices performing processing of data according to a program (a set of instructions) automatically, i.e. without human intervention. The data are to be exchanged over the network. The definition is not marginal, since last year a Court in the Netherlands ruled that breaking into an encrypted wi-fi network was legal, because access was gained through a router, which fails to meet the Dutch definition of computer.[190] According to the Court, routers process and transfer data, but do not store them; nevertheless, they are computer in the sense of the Convention, whose main feature is the 'automatic processing of data'. The case is going to be reviewed by the High Court of the Netherlands. Pursuant to article 4, the application of specific technical tools like cookies or botnets,[191] which can lead to illegal access, is not considered unlawful *per se*, if their instalment has not been rejected by the website owner. This provision is particularly worrying today, as most cyber-attacks are allowed by botnets, and building a bot requires to commit the crime identified by article 4. Furthermore, the use of cookies for the purposes of behavioural advertising is rarely visible, and therefore consensual. Since white-hat hacking (that is, the probing of a system or program to discover

---

[187] Brenner, *The Council of Europe's Convention on Cybercrime.*

[188] Ibid.

[189] Cybercrime Convention, *Explanatory Memorandum*, p. 31.

[190] Loek Essers, "Dutch Court Rules WiFi Hacking Is Now Legal", *Pcworld.com*, 18 March 2011and EDRi-gram, N. 9.6, 23 March 2011.

[191] That is, the distributed network of virtually kidnapped private personal computers (zombies) by criminal organizations/individuals used to perpetrate large-scale cyber-attacks. Porcedda, *Transatlantic Approaches to Cybersecurity*. See also *supra*, note 106, p. 22.

vulnerabilities and fix them), could be considered an offence in the terms of this provision, the drafters allow states to introduce additional requirements to attach criminality. Yet, certain states may criminalise it nonetheless, thus undermining one of the most effective ways to avoid the so-called 'zero day exploits attack'.[192]

Article 3 criminalises illegally intercepting, i.e. listening, monitoring, surveillance or procuring, by technical means (any computer systems or electronic eavesdropping/tapping devices, fixed or wireless, by recording or using softwares/codes/passwords), computer data not publicly transmitted[193] to, from or within a (single, two, etc.) computer system, including electromagnetic emissions (radiations) from a PC carrying computer data. Indeed, exploiting electro-magnetic pulses can be used to perpetrate an offence physically.[194] While the emissions are not considered data, they can lead to reconstructing the data, whereas radio transmissions eavesdropping criminalisation is excluded. As clarified by the Explanatory Memorandum, the objective is to protect the right to privacy of any electronic data communications pursuant to article 8 ECHR. However, Wi-Fi connections are established by means of radio waves, often unencrypted. In 2010, ruling on an intellectual property lawsuit, the Federal Supreme Court in Germany fined a man for failing to properly ensure his Wi-Fi network. As a consequence of his negligence, a third party was able to download a song and share it illegally on the Internet. A similar case in Denmark led to an opposite decision.[195] The question is going to gain increasing importance in relation to the Google Street View affair. According to a recent report,[196] the company has run for four years a scheme to collect as much personal information from household's Wi-Fi connections as possible, in what has been dubbed the "single greatest privacy breach in history."[197] Google Street cars stole the 600 GB of data in conjunction with their mapping of world's cities, alongside capturing images of each street. Data included, *inter alia*, email login information, email conversations, passwords, URLs of visited websites etc. In 2011, CNIL, the French DPA, fined Google € 100.000 for its the massive interception of personal data;[198] investigations are now bound to be resumed in the EU,[199] and the ensuing cases may lead to interesting conclusions, regardless the infrastructure used for the connection.

Article 4 on data interference grants protection to stored computer data (or programs), akin to corporeal objects, against intentional damage, deterioration, deletion, suppression and alteration. Damaging and deterioration refer to the negative modification of the integrity or of information content of data programmes; deletion means the destruction of objects, which makes them unrecognisable; suppression denotes unavailability of the data to the user, or the data carrier containing it; finally, alteration stands for modification. This provision covers viruses[200] and malware[201] in general, including root-kits[202] and Trojan horses, i.e. malicious software used to take

---

[192] Those attacks that exploit undiscovered bugs in software, from which comes the importance of testing.

[193] The data itself can be public, but the users may want to communicate it privately. This includes communications of employees, as in ECHR Judgement in Halford v. UK case, 25 June 1997, 20605/92.

[194] EMPS, bursts of high-energy radiation destroying the chips of affected PCs caused by a remote cyber-attack.

[195] See at European Digital Rights (EDRi) "German Supreme Court Fines Owner Of Open WiFi Network", Edri-gram, 22 May 2010.

[196] Charles Arthur, "Google's problem is that it now believes itself above others – even government," *Guardian.co.uk*, 1 May 2012; David Streitfeld and Kevin J. O'Brien, "Google Privacy Inquiries get little cooperation," *Nytimes.com*, 22 May 2012.

[197] Asher Moses, " 'Petulant' Conroy accuses Google of 'single greatest privacy breach'," *Smh.com.au*, May 25, 2010.

[198] Commission Nationale de l'Informatique et des Libertés (CNIL), "Google Street View : CNIL pronounces a fine of 100,000 Euros", 21 March 2011.

[199] Kevin O'Brien, "European Regulators to reopen Google Street View inquiries," *Nytimes.com*, 1 May 2012.

[200] Cybercrime Convention, *Explanatory Memorandum*, par. 61.

[201] The difference between worms (self-spreading) and viruses (requiting user intervention) is blurring, and the term malware is being used instead. House of Lords, "Personal Internet Security."

possession of a computer and create a botnet. Said deeds could be intentional and with right in case of design and commercial practices, such as testing or reconfiguring an operating system which automatically disables previous software. As for encryption (which enables anonymity or protects content), it is considered legitimate for privacy purposes. However, its abuses, such as altering the packet header information to mislead the origin of the communication (which is crucial for anonymity), can be considered unlawful. States can apply a reserve of serious harm.

Article 5 on system interference protects the legal interest of operators and users to have a system functioning properly. It forbids serious hindering of a computer system – that is, serious interference through inputting, transmitting, damaging, deleting, deteriorating altering or suppressing computer data. This article covers DoS, viruses that slow down or prevent the operation of a system, and programs sending a large amount of mails that block the ability to operate (spamming), which can be perpetrated by means of a botnet. Testing and reconfiguration, as examples of operational or commercial practices, are excluded. States may define it as an administrative offence. The abovementioned Stuxnet is covered by both articles 4 and 5.

Article 6 on misuse of devices addresses the offences in articles 2 and 5 at the source, since committing them requires the possession of some kind of hacker tools, or means of access available on the black market.[203] It prohibits the production, sale, procurement for use, import, distribution (forwarding to others) or making available of (placing devices online, including hyperlinks or compilation of hyperlinks): a device (also computer program, such as viruses or programs that allow access to take place) designed or adapted primarily for committing the offences in 2-5 (dual-use devices are explicitly excluded); a computer password, access code, or similar data allowing to access whole or part of a computer system to commit any of the crimes from 2-5; possessing one, or a number (subject to states' decisions), of the above items for committing any of the offences above. The above does not cover testing (cracking devices) the protection, counter-attacks against computer systems and network analysis devices. States may decide not to apply these provisions, provided they criminalise selling, distributing and making available of computer passwords, access code and similar data.

Title 2 refers to computer-related offences, which, according to the drafters, "play a greater role in practice."[204] Article 7 on computer-related forgery establishes an offence akin to tangible documents forgery, since the manipulation of electronic data (public or private document) with evidentiary value (legal effects) may have the same consequences in misleading a third party. The article outlaws "the (unauthorized) input, alteration (modification), deletion (removal) or suppression (concealment) of computer data" so that data is inauthentic (referring as a minimum to the issuer of the data), but with the objective of making it seem authentic for legal purposes (referring to legal transactions and legally relevant documents), independently from the fact that the data is readable and intelligible. States may require the condition of dishonest intent.

Article 8 proscribes "any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property". The provisions covers credit card fraud and frauds "to assets represented or administered in computer systems."[205] There must be the "fraudulent and dishonest" intentionality to cause an economic benefit for oneself or another person, with a corresponding loss of property (in the form of tangibles, intangibles and money) to another one (i.e., a zero-sum outcome). The use of 'bots' to collect commercial data and compare prices, which may cause advantage to some and disadvantage to others, is not criminalised. Computer-related fraud must be done either via the input, alteration, deletion or suppression of computer data (as in previous articles, but referred to the

(Contd.)

[202] A piece of malware very well hidden in the operating system.

[203] As addressed by CoE ETS N. 178 and Directive 98/84/EC, and also the 1929 Geneva Convention on Counterfeiting.

[204] Id., par. 35.

[205] Id., par. 86.

object in question, such as hardware manipulations, acts affecting recording or flow of data, etc.); or any interference with the functioning of a pc system (to supplement the above).

Title 3 only deals with a specific content-related issue: offences related to child pornography. This provision outlaws: producing (to combat the dangers at their source); offering (soliciting others) or making available (creating websites or hyperlinks of websites); distributing (active dissemination) or transmitting (sending material); procuring for oneself or another person (actively obtaining, i.e. by downloading it); and possessing (since it stimulates demand) child pornography, namely (realistic images representing) a minor (proper child), a minor and a minor, a person appearing as a minor in sexually explicit conduct (oral/anal/genital contact or representation of the genital, bestiality, masturbation, sadistic or masochistic abuse), through a computer system. 'Minor' has to be intended in the sense of sexual object and not of consent for sexual intercourse. States may reserve not to apply the procuring for oneself and others of child pornography and exclude (unrealistic images) of a person appearing as a minor engaged in sexually explicit conduct as child pornography. Liability does not attach when providers act as 'mere conduit', and medical, scientific and artistic purposes are considered legal. In addition, if the person involved appears not to be a minor, criminal liability does not apply (the article takes into account the right to privacy and freedom of thought and expression).

Finally, title 4 covers offences related to infringements of copyright, which seem the most common form of crime, and related or neighbouring rights. Literary, photographic, musical, audio-visual etc. works are covered by the article, provided that the persons qualify as right holders. Patents and trademark-related violations are not included as they are addressed by other instruments. Criminalisation covers infringement (as defined by each state) of copyright and neighbouring rights (those covered by the copyright), when the acts are done wilfully, on a commercial scale, by means of a computer system. In any case, criminal law defences apply when actions are done with right. States may limit responsibility under this article, if other remedies (civil or administrative measures) are available and the reservations do not impact negatively on relevant international obligations.[206]

Article 11 (Title 5), outlaws aiding and abetting, and even the attempt to commit the offences identified in the Convention. It clarifies that the mere conduit by service providers of malicious code or harmful content data cannot constitute a crime, and the providers cannot be held liable, nor are they obliged to actively monitor the content of the Internet to spot criminal activities. Nonetheless, the article is subject to reservations to whole or part of it, to allow the widest ratification possible, given the disagreement on what crimes can be attempted, and the differences in the legal traditions of the parties.

Article 12 provides states with the possibility ('should' is used instead of 'shall') of introducing corporate liability, i.e. liability of legal persons (corporations, associations and the like), when four conditions apply: (i) one of the crimes listed by the Convention occurs; the action was committed (ii) for the benefit of that legal person and (iii) by a natural person who has a leading position within the legal person; (iv) said person, acting as an individual or as a representative of the legal person, has acted on the basis of either (a) a power of representation or (b) the authority to take decisions or (c) to exercise control.

Liability is further extended when three conditions apply: (i) the crime is committed by an employee or agent who is under the control or supervision of the natural leading person in paragraph one, i.e. acting within the scope of the leading persons' authority; (ii) the latter fails to supervise or control an employee or agent; (iii) and the crime generates a benefit for the legal person. The failure of supervising and controlling includes taking appropriate measures to prevent the crimes, but does not amount to an obligation to watch the communications of the employees and, in any case, varies according to the type of legal person.

[206] Namely Article 61 of the TRIPS Agreement.

Pursuant to Article 13, states must introduce sanctions that are effective, proportionate and dissuasive, including the deprivation of liberty for people and monetary sanctions for legal persons, to ensure the effectiveness of the Convention.

Similar to the procedural provisions, there are a number of weaknesses to be discussed. Firstly, the text – self-confessedly – does not address all forms of possible crimes (it leaves out theft, extortion,[207] stalking, terrorism, psychological injury infliction, among others) committable by means of a computer system, without giving an explanation as to why only a sub-set of the traditional crimes committable via a computer system, specifically fraud, forgery and child pornography was chosen.

Secondly, no provision explicitly condemns the violation of data protection rules.[208] While article 3 refers to the protection of privacy (but only in the explanatory memorandum), and article 5 forbids spamming (when it causes interference), the procedural laws significantly water down the protection available. This denies the link existing between certain forms of crime and data protection, and is likely to cause confusion as to which law should apply in the case of certain violations.

Thirdly, one of the purported objectives of the treaty, namely to harmonise the laws, not least to limit the creation of cyber havens, is betrayed by two factors. On the one hand, while the Convention follows in the tracks of the US legal framework,[209] it does not offer model legislation for countries to follow when implementing it. On the other hand, the substantive provisions offer states room of manoeuvre not to impose liability.[210]

Finally, notwithstanding the fact that the drafters admit that the most effective means of preventing unauthorized access is the introduction and development of effective security measures, the Convention adopts a traditional approach only, whereby cybercrime is criminalised by means of national legislation, which sets up tools and procedures allowing its detection, investigation and prosecution. Yet, this traditional nation-based approach may not work; the Convention disregards the fact that cyberspace allows individuals to remotely exploit any country's citizens,[211] thus overlooking the problem of attribution. Hence, the Convention truly appears to be written by LEAs for LEAs, and it seems better placed to address more traditional forms of crimes, such as child pornography and copyright, while failing to address non-traditional forms of cybercrime.

3.2.3 The additional Protocol on acts of a racist and xenophobic nature committed through computer systems

The possibility to criminalise racism and xenophobia was discussed at length, but its introduction was refused on freedom of expression grounds. Therefore, these acts are treated in a dedicated Protocol, whose adoption was recommended by the Parliamentary Assembly, and endorsed by the Council of Ministers. The purpose of this protocol is twofold. First, to harmonise the substantive criminal law in the fight against racism and xenophobia on the Internet, by giving common responses to the developments of the new technologies. Secondly, to improve international cooperation in this area of crime prevention, by taking advantage of the mechanisms established by the Cybercrime Convention. The Preamble expresses the need to ensure a proper balance between the freedom of expression,

---

[207] Cyber extortion is usually perpetrated via a botnet delivering a DoS attack, followed by an offer of consultancy services to remove the problem; the victims, typically online gambling sites, often prefer to pay the ransom without reporting. Sommer and Brown, *Reducing Cybersecurity Risks*.

[208] Article 29 Data Protection Working Party, WP 41.

[209] In fact, the Convention was immediately ratified, without needing additional laws, as it was considered self-enforcing. Brenner, "The Council of Europe's Convention on Cybercrime."

[210] Ibid.

[211] Ibid.

whose established principles are not affected, and the contrast to acts of a racist and xenophobic character as a violation of human rights. To do so, it builds on existing international agreements.[212]

Racist and xenophobic material are defined in article 2, and further clarified in the Explanatory Memorandum to the Protocol.[213]

Chapter 2, titled 'Measures to be taken at the national level,' covers the substantive law issues relating to the subject matter of the Protocol, and identifies four offences, which, like the ones listed in the Convention, must be perpetrated 'without right' and 'intentionally' (the exact meaning thereof being left open to national interpretation), thus excluding lawful state conduct, common operating business practices and system design.

Article 3 condemns the dissemination of racist and xenophobic material through computer systems. It refers to the distribution (active dissemination) or making available (posting or compilation of hyperlinks) of racist and xenophobic material to the public, through a computer system. Private communications, whose nature is usually notified by the intention to deliver the message to a pre-determined receiver, are excluded, whereas the use of a chat room to exchange material could be deemed public.

Article 5 equally excludes private communications. Accordingly, racist and xenophobic insults, i.e. insulting (any expression prejudicing the honour or dignity) publicly, through a computer system, persons or group of persons, for the reason that they belong to a group identified by colour, race, decent, national/ethnic origin or religion, is outlawed.

The private or public nature of the communication makes no difference, on the other hand, for racist and xenophobic motivated threat (article 4). It consists in threatening (menace) the commission of a serious criminal offence as determined in domestic law, through a computer system, a person or a group of persons only on the basis of their belonging to a group identified by colour, race, descent, national/ethnic origin or religion.

Article 6 on denial, gross minimisation, approval or justification of genocide or crimes against humanity mirrors article 3. It forbids the distributing or making available through a computer system to the public, material which denies, grossly minimises, approves or justifies genocides or crimes against humanity, as recognised by the special tribunals instituted to address them (and not only limited to Nazi crimes). The provision applies also to future crimes against humanity, provided that the party signing the Protocol recognises the court establishing them.

Finally, article 7 criminalises aiding and abetting of the offences above. Differently from the Convention, the attempt to commit the crimes in here is not criminalised. More strikingly, though, articles 3, 5 and 6 allow substantive reservations, and in particular the right not to apply them in part or in whole, on grounds that the conduct has to lead to serious hatred, violence, or great distress for the victim (articles 3, 5 and 6), or the state lacks the effective remedies because of the established principles of its legal system concerning freedom of expression (article 3).

---

[212] For instance, the ECHR and its Protocol n. 12, and the UN Convention on the Elimination of all Forms of Discrimination (1965). See Morten Kjaerum, "Combating Racial and Related Discrimination," in *International Protection of Human Rights: A textbook*, ed. Catarina Krause and Martin Scheinin (Turku: Abo, 2009).

[213] They refer to any material, in any format which can be stored, processed and transmitted by means of a computer system, which leads to either advocating (plea in favour of), promoting (encourage), or inciting (urge), both hatred (intense dislike or enmity), discrimination (a different unjustified treatment given to somebody or a group solely on the basis of certain characteristics, to which the classical ECHR test applies) and violence (unlawful use of force). Such actions have to be directed against an individual or a group of people, based on race, colour, descent (descending from people having certain race or colour; which is different from social origin), national or ethnic group (regardless of the actual legal possession of a certain nationality), and religion (conviction and beliefs) when it is used as a pretext for any of these factors.

Chapter 3, article 8 establishes the relationship with the Convention, and in particular the application, *mutatis mutandis*, of articles 1, 12, 13, 22, 41, 44, 45 and 46 of the Convention. The scope of application of articles 14 to 21, and 23 to 25, can be extended to articles 2 to 7 of the Protocol.

3.3 The Council Framework Decision on Attacks against Information Systems and the Proposal for a New Directive

3.3.1 The Council Framework Decision on Attacks against Information Systems

The Council Framework Decision on Attacks against Information Systems was adopted with a view to pursuing cooperation between the competent authorities in the area, by means of approximating criminal substantive law beyond the Cybercrime Convention and the work carried out by the G8, as recalled in section 2.3.3. The Council Framework Decision's comprehensive approach was clearly inspired by the documents referred to therein. The rationale for its adoption was the evidence of the increasing attacks against information systems, as a particular expression of organised crime or terrorism. There are both similarities and differences between the Council Framework Decision and the Cybercrime Convention.

As for similarities, criminalisation attaches to certain conducts only when committed without right, meaning that the access or interference must be prohibited by national law, or without authorization, and intentionally. Article 2 on illegal access to information systems, article 3 on illegal system interference and article 4 on illegal data interference mirror articles 2, 5 and 4 of the Cybercrime Convention respectively. Moreover, criminalisation attaches to cases that are not minor, with a view to avoid over-criminalisation.

As for differences, the Framework Decision lays down that authorised testing or protection of information systems cannot be criminalised. Article 5 criminalises instigation of, aiding and abetting, as well as attempting to commit the offences in articles 2 to 4, without any reservations (apart from the attempt to commit the offence in article 2, i.e. illegal access to information systems). In addition, article 6 addresses penalties, which must be effective, proportional and dissuasive, and amount to a maximum of 3 years of imprisonment. Two aggravating circumstances are established, leading to more severe penalties (article 7), namely when the action is committed within the framework of a criminal organisation, and if the action has caused serious damage or affected essential interests. Furthermore, article 8 envisages an obligation for MSs to introduce liability for legal persons, in parallel to criminal liability against natural persons, for the same reasons established by article 12 of the Cybercrime Convention. Accordingly, article 9 establishes the penalties for legal persons held liable pursuant to article 8(1). Article 10 addresses rules to establish jurisdiction and govern extradition. Finally, article 11 regulates the exchange of information, clearly referring to the respect of data protection rules, namely Convention 108, as clarified in the Preamble.

The rationale for repealing the Framework Decision is illustrated in the report on its implementation, published in July 2008, which highlighted two problems. Firstly, the implementation was not complete, (the deadline being the March 2007).[214] Secondly, new threats had emerged, such as large-scale attacks, namely "those attacks that can either be carried out with the use of tools affecting significant numbers of information systems (computers), or attacks that cause considerable damage, e.g. in terms of disrupted system services, financial cost, loss of personal data, etc.,"[215] and botnets. The text, therefore, approximated the laws to a limited extent, and did not take into sufficient account the gravity of the crimes.

[214] The following states have not taken any action towards the Decision: Cyprus, Ireland, Greece, Italy, Slovakia and the UK.

[215] European Commission, COM (2009) 149 final, p. 3.

3.3.2 The 'Proposal for a Directive on Attacks against Information Systems'[216]

There was therefore consensus towards overhauling the Council Framework Decision, to introduce common provisions "to prevent such attacks and improve European criminal justice cooperation in the field" (article 1), based on the growing critical function for the public or the private sector performed by information systems, which are suffering increasingly sophisticated attacks by organised crime, terrorism, and even politically motivated actions.[217] The proposal intends to further harmonize laws and establish penalties, address the lack of reporting and the fact that not all MS had signed the Cybercrime Convention, to which the EU is not a signatory. Content-wise, the proposal partly builds on the Decision and partly innovates.

As for the parts building on the Decision (and therefore on the Cybercrime Convention) criminalisation attaches only to cases committed intentionally, and which are not 'minor' (although *in abstracto* criminalisation would attach). In addition, the definitions (article 2) and a number of articles remain unvaried, namely: illegal access to information systems (article 3, but without reservation) illegal system interference (article 4), illegal data interference (article 5), aiding and abetting (article 8), liability of legal persons (article 11) and penalties on legal persons (article 12). Penalties (article 9) are redefined and increased. Moreover, "committing the crime against a critical infrastructure information system" is added as an aggravating circumstance (article 9 or 10).[218]

As for innovations, the proposal includes the offence of illegal interception (article 6), namely the intentional "interception by technical means, of non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data." Then, article 7 prohibits "the production, sale, procurement for use, import, possession, distribution or otherwise making available: A) a computer program, designed or adapted primarily for the purpose of committing any of the offences in 3-6 and B) a computer password, access code or similar data". Furthermore, article 14 provides that, "for the purpose of exchanging information relating to the offences 3-8, MSs shall make use of the existing network of operational contact points" established by the G8 and by the Convention. It is interesting to note that the phrase "in accordance with data protection rules", which was included in the previous version, has been removed. The Preamble clarifies that personal data collected in the course of actions pursuant to the Directive should be handled according to Council Framework Decision 2008/977/JHA, apart from those falling within the scope of Regulation 45/2001. The reference is legally correct, but probably will be out-dated by the revision of Directive 95/46/EC, as I will address in section 4.4.

---

[216] European Commission, COM (2010) 517 final; Council. *Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, replacing Council Framework Decision 2005/222/JHA.* 11566/11, Brussels, 15 June 2011.

[217] Motivations have evolved over time. At the beginning, the average perpetrator was the lonely tech-savvy desiring to attract the attention for various reasons, from disgruntlement as in the case of the Love bug, through being hired (the Gorshov case) and earning the fame before the cyber-community, to testing the system, as is the case of the white-hat hackers. Yet, the profile seems to have evolved in parallel with the possible monetary gains. It seems that cybercrime has attracted the attention of organized crime, such as Russian Mafia, which has become refined in the means (i.e. managing different languages) and scale. A proper criminal industry producing malware seems to be emerging, which reduces the marginal costs and increases the benefits of the supply of crime. For instance, botnets can be bought (for as cheaply as $0.04 per member bot in 2008) and easily managed, so that even people with limited technical knowledge can create and use botnets. In addition, criminals often join forces: for instance, the US mafia cooperates with the Russian criminal gangs and rogue ISPs to extort online gambling sites and produce child pornography. Sommer and Brown, *Reducing Systemic Cybersecurity Risks*.

[218] Also, the reference to the definition of organised crime is updated, as defined by the Council Framework Decision 2008/841/JHA; Framework Decision 2009/948/JHA on the prevention and settlement of conflict of jurisdiction in criminal proceedings becomes the base for coordinating prosecution; and the rules on jurisdiction (article 13) are slightly modified.

However, these three articles do not properly innovate, in that they are taken from the Cybercrime Convention. The only original addition is article 15, which provides for the establishment of "a system in place for (the) recording, production and provision of statistical data". The rationale, as clarified in recital 12, is to have a better picture of the situation, in order to help Europol or ENISA assess the extent of cybercrime and network information security in Europe.

The content of the Decision is likely bound to change, but appraising it is already possible. While the Decision clearly builds on the Cybercrime Convention, it addresses (some of) its shortcomings in five respects. First of all, states are explicitly discouraged from adding additional conditions to the provisions, thus aiming at a higher level of harmonization.[219] Secondly, the collection of statistical evidence becomes mandatory, which will certainly contribute to a better understanding of the problem and, hopefully, to better policies. Thirdly, it explicitly criminalises the use of botnets. Fourthly, and very importantly, it only deals with non-traditional cybercrimes. Finally, the text addresses the fact that large-scale attacks are essentially the same types of crime on a bigger scale, and marks the difference in terms of gravity of the penalty.

The Explanatory Memorandum to the proposal clarifies that the text is compliant and consistent with "EU policies on combating organised crime, increasing the resilience of computer networks, protecting CII and data protection. The objectives are also consistent with the Safer Internet Programme which was set up to promote safer use of the Internet and new online technologies, and to combat illegal content."[220] In accordance with the three-pronged approach, the Communication recalls that botnets are prohibited under privacy and data protection rules (e-privacy), as well as the interception of communications on public communications services without the consent of the user/legal authorization, and that national administrative agencies are cooperating under the European contact network of Spam authorities. Furthermore, recital 16 declares that the Directive "respects the fundamental rights and observes the principles recognised in particular by the EUCFR, including the protection of personal data, freedom of expression and information, the right to a fair trial, presumption of innocence and the rights of the defence, as well as the principles of legality and proportionality of criminal offences and penalties."

However, there are a number of weaknesses. The only reference to data protection is contained in recital 15, whereby the personal data processed in the context of the implementation of the Directive should be protected in accordance with the rules laid down in Council Framework Decision 2008/977/JHA, which has many shortcomings as addressed in section 4.4.7, and Regulation 45/2011/EC. The reference to data protection rules in article 14 has been removed. Moreover, the Preamble does not recall the three-pronged approach, but just the fact that loss of personal data could represent a serious damage in certain MSs (recital 3). Actually, the very reference to the Cybercrime Convention contradicts such connection to the three-pronged approach, due to the shortcomings relating to its procedural law and the particular consideration of human rights. Indeed, the first draft is closer to the Cybercrime Convention than the Decision as far as privacy and data protection are concerned, in that it only recognises such rights in the Preamble.

Finally, although the proposal's purpose is to lay down preventive rules, the only prevention is the deterrence created by harsher penalties. It does not introduce any technical preventive measure, nor it envisages means to distribute responsibility among actors different from users (i.e. ISPs and services). In other words, the Directive still takes a criminalisation stance, and misses the point of the importance of prevention.

---

[219] An interesting question concerns whether the use of the opt-out options available to some countries would actually lead to the creation of data havens.

[220] These include the 'prevention of and fight against crime', 'criminal justice', 'safer internet,' the 'critical information infrastructure initiative,' Framework Decision 2004/68/JHA on Combating Sexual Exploitation of the Children and Child Pornography. European Commission, COM (2010) 609 final, 4 November 2010, p. 4.

3.4 Questions of Definitions

3.4.1 Cybercrime

The legal instruments above try to address the problem of harmonising definitions. It is now the time to discuss the conceptual problem in greater detail. Cybercrime is a 'term of hype' encompassing the following:

- Compromising computer systems, by logical means (software) such as: key loggers[221] or other spy-ware; viruses and (embedded) malware; root-kits; zero day exploits attack; logic bombs and Trojan horses. The offence can also take place physically, such as exploiting electro-magnetic pulses.
- Attacking individuals or groups of individuals, either for economic or other purposes: identity theft realized through phishing and pharming leading to financial (bank) fraud;[222] cyber-bullying; e-stalking; child pornography; racist and xenophobic speech; e-blackmailing; and loss of confidentiality. Many of these attacks are perpetrated by means of social engineering. The user is induced to trust the source of the message, its content or both, and to follow the instructions contained in the message, usually a request to provide certain data or to install malware.
- Offences to businesses: copyright infringement; e-extortion; e-espionage; hacktivism by means of DoS, DDoS or websites defacement; spoofing;[223] data breach to acquire financial information; and synthetic id fraud.[224] The latest noteworthy case of the former was the two data breaches suffered by Sony in 2011.[225]
- Offences to state: cyber-terrorism;[226] attacks to the CII, or the Critical National Infrastructure; e-espionage;[227] 'hacktivism'[228] by means of Dos or DDoS or websites defacement.

Some of these offences perpetrated in a wider scale are addressed as large-scale cyber-attacks. Unsurprisingly, therefore, the Convention's substantive choice has been criticised, and several alternative taxonomies have been proposed. One hinges on the intention behind cybercrime, and distinguishes between:

- Targeted (specific tools, often requiring high expertise, against specific targets, with the objective of doing serious damage) vs. opportunistic (diffused, doing individually less damage) attacks;
- Predatory (the aim is to damage someone or their property, leading to some form of wealth redistribution) vs. market-based (generate new income, i.e. selling drugs online).[229]

---

[221] Software which can detect the keys pressed, and therefore the passwords used.

[222] "Money mules", i.e. fake bank accounts obtained by assembling fake identities with details of various people, are often used to hide the destination of funds. Sommer and Brown, *Reducing Systemic Cybersecurity Risks*.

[223] When one masquerades oneself as another person.

[224] The combination of pieces of different true identities to obtain a new one. Kshetry, *The Global Cybercrime Industry*, p. 5.

[225] Maria Grazia Porcedda, *Reviving Privacy: the Opportunity of Cyber-security*, Proceedings of the VIII International Conference on Internet, Law and Politics (IDP 2012), Barcelona, forthcoming.

[226] It is a controversial term, which needs "to be defined with the same precision as other forms of terrorist crime. There must be an intention and a real risk of causing death or serious bodily harm among members of the public, plus a terroristic intent, either to cause fear among the population or to compel the government to do or not to do something." Martin Scheinin in United Nations, *Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes*. New York: Counter-Terrorism Implementation Task Force (CTITF), 2009.

[227] According to Sommer and Brown, e-espionage is old wine in new bottles. To be effective, espionage does not need being technologically sophisticated.

[228] Hacking (web defacement or DDoS) for political reasons, i.e. the case of the Anonymous group.

The US Department of Justice has developed a tripartite understanding of cybercrime, which has also been used in the UK, Australia and Canada: i) the computer or the networks is a target (true computer crime); ii) the PC is a tool (facilitated crime); iii) the PC is an incidental aspect of the commission of the crime (computer supported crime).

Moreover, the 2004 G8 Government and Industry Conference on High-Tech Crime recommended the adoption of a threat-focused classification,[230] which distinguishes between:

- Computer infrastructure attacks: "Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Malicious acts, unauthorized access, theft of service, DoS"; and
- Computer assisted threats: "malicious activities (e.g. fraud, drug, trafficking, money laundering, infringement to intellectual property rights, child pornography, hoaxes, gathering of information, and illegal copy of data)."[231]

These taxonomies confirm once more what was pointed out in the policy documents, notably that cybercrime encompasses both "online" and "offline" crimes, i.e. crimes that would exist only online (narrow cybercrime), and crimes that exist also in the off-line world (broad cybercrime), respectively.[232] It has been argued that drawing a line between cyber space and the real world could be risky, because the latter may well suggest useful solutions, in that some 'off-line' cybercrimes are strongly related to the offline world (i.e. cyber-bullying). Accordingly, the Internet could be treated like a public space and informed by the principle that, 'if it is stupid offline, it is also online', and this interrelation could be considered in technological issues.[233] This is why some consider that reaching a final definition of cybercrime is unrealistic, and that the term should be understood broadly, in a way that emphasises the importance of technology in these acts.[234] Yet, the fact remains that there are important features, which such a comprehensive definition hides. Let us take the following taxonomy, which distinguishes:

- The security of ICT systems, including: personal security, computer security, network security, national security, digital identification and authorisation, tracking network traffic across borders and jurisdictions, data protection, intellectual property right protection on digital media; from
- Safety to people, including: the protection of children using the internet and mobile cell-phones; family/school/community/responsibilities; paedophilia; cyber-bulling; digital dossier recording details of an individual's life; addiction to online games; suicide and self-harm websites."[235]

According to the authors of this taxonomy, the two groups of threats are tackled by two overlapping, but different 'communities', which bear distinctive cultures:

> "Safety to people has become associated with the activities of NGOs, government agencies, experts, local groups and other stakeholders whose policy agendas prioritise issues of personal safety and harm in online worlds, particularly those concerning children. […] An equivalent cyber-security community has evolved over a longer period of ICT development, anchored in

(Contd.)

[229] Kshetri, *The Global Cybercrime Industry*.

[230] Ibid..

[231] G8 Government and Industry Conference on High-Tech Crime, Report of Workshop 3, "Threat Assessment and Prevention," Tokyo, 22-24 May 2001, available at <http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-6.html> (last accessed on 23 July 2011).

[232] Clough, "Principles of Cybercrime."

[233] Nash and Peltu, "Rethinking Safety and Security in a Networked World."

[234] Clough, "Principles of Cybercrime." Indeed, policy approaches, including technological choices, are conditioned by local cultures, where the same terms have different emotional impact and significance (Nash and Peltu, "Rethinking Safety and Security in a Networked World").

[235] Nash and Peltu, "Rethinking Safety and Security in a Networked World," p. 7.

> more technical, institutional, economic and regulatory concerns, such as safeguarding network, business and government infrastructures."[236]

These cultures argue for different measures. For instance, the social pressure to counter child pornography and, to a lesser extent but probably more efficiently, intellectual property violation, translates into lobbying hard for the introduction of the habit of content filtering (that is, the curbing of net neutrality), usually carried out by ISPs.[237] ISPs already carry out filtering for network security purposes, meaning to protect their own network from malware, which is both lawful and welcome (although critics maintain that this can curb innovation).

Here, the problem is that "in the online environment, what constitutes content is difficult to recognise: it's all code, whether it is a virus,[238] a political speech, or an image with child pornography.'[239] Therefore, filtering can be theoretically applied for any purposes, be it good or bad, from malware detection to surveillance (usually with the support of social techniques). Moreover, filtering in general can be detected and bypassed, sometimes quite easily, and is exposed to false positives and negatives. The application of filters may lead offenders to use peer-to-peer instead, where content filtering is of no use, or the dark net.[240] In order to be effective, filtering should be applied at the end points of any communication, which means that users should be in charge of the final decision. This seems unrealistic; while expert users may accomplish the task well, beginners and unaware users are generally unable to recognise the risks and taking countermeasures. Unfortunately, the difference between expert and non-expert users is poorly addressed.[241] This places ISPs in a better position to do so;[242] ISPs are actually using filtering techniques for traffic management purposes.

The issue is, there are several types of filtering,[243] each of them accomplishing different kinds of results, and having different impacts. "Certain inspection techniques involve the monitoring of content of communications, websites visited, emails sent and received, the time when it takes place, etc., enabling filtering of communications."[244] Content filtering of the type required by anti-child pornography and pro-intellectual property lobbies requires deep packet inspection, which is extremely intrusive from the point of view of privacy and data protection. In particular, it affects the confidentiality of communications, which is protected by article 8 ECHR and the related jurisprudence, articles 7 and 8 of the EUCFR, as well as by article 5 of the e-privacy Directive.[245] This means that employing the most intrusive types of filtering requires a very strong oversight, to avoid unjustified purpose creep. The problem is that filtering is becoming commonplace for a host of services. A way to counter the practice would be to use end-to-end encryption, which is nonetheless a double-edged sword. On the one hand, it shields users against several cybercrimes, such as illegal

---

[236] Ibid.

[237] House of Lords, *Personal Internet Security*.

[238] This means that filtering can be exercised for cyber-security purposes, which has been criticised by some as it may lead to the inhibition of the development of new protocols and applications.

[239] House of Lords, *Personal Internet Security*, p. 23.

[240] Ibid.

[241] Nash and Peltu, "Rethinking Safety and Security in a Networked World."

[242] ISPs, for instance, are active in the detection of botnets; an example is the German anti-botnet initiative (see at http://www.oecd.org/dataoecd/42/50/45509383.pdf).

[243] These include: TCP/IP header filtering; TCP/IP content filtering; DNS tampering; HTTP proxy filtering; hybrid TCP/IP and HTTP Proxy filtering; denial of service; domain deregistration; and server take down (Steven J. Murdoch and Ross Anderson, Tools and Technology of Internet Filtering." in *Access Denied: The Practice and Policy of Global Internet Filtering*, edited by Ron Deibert et al. (Cambridge: The MIT Press, 2008.)).

[244] EDPS, *Opinion on Net Neutrality*, p. 2.

[245] Ibid.

interception, illegal access and fraud, and protects privacy and the personal data. On the other, it is unwelcome by LEAs, because it could hide criminal activity.

Protecting the victims of child pornography is a legitimate end, but it is necessary to assess how the practices used to uncover the culprits are affecting the prevention and investigation of other types of cyber-crimes. Before drawing conclusions, an additional step in the discussion is needed.

3.4.2 Cyber-security or Technical vs. National Security Communities

The argument of the existence of two macro communities bearing different cultures can be integrated and refined with the idea that further divisions exist within communities. In particular, in the community addressing the security of ICT systems, there would be a difference between "one, focusing on individual systems and networks, has its roots in computer science and engineering communities; the other, a more recent concern, focuses on collective and institutional systems, reflecting the influence of political and national security actors." [246] These two communities hold two definitions of security, bearing different moral claims, and leading to different policy and technology outcomes, namely prevention or punishment. This is feasible, since technology can accommodate any needs.[247]

The technical community focuses on a broad variation of individual harms: damage to property, autonomy, privacy and productivity. Indeed, from a technical point of view, security is typically intended in terms of integrity, confidentiality and availability of the service, privacy being a subset of confidentiality, which means it is embedded in the concept of technical security (and vice versa, as shown in the privacy chapter). This community responds with pre-emption reinforcing each node – the individual. In fact, online crimes (i.e. illegal access, illegal interception, data interference, system interference and misuse of devices) largely depend either on the fact that individuals' computer systems and data lack sufficient protection, such as encryption, firewalls and antivirus software, run outdated programmes exposed to bugs and exploits, or that on users are unaware and vulnerable to social engineering. Also computer-related forgery and fraud could be avoided by higher protection of the individual: if the data, the system, and the communications are protected, the odds of an incident are reduced. The point is, these are the measures ensuring a high protection of privacy. Logically, the opposite has to be true: by adopting the necessary measures to protect one's privacy, one's security is highly ensured. Highly, not completely, because other individuals play a role at a higher level: the ISPs providing the networks, which are in charge of their security, and the businesses offering their products to the market, products which should be as safe as possible. Yet, in the EU, the security of the network, and the incentive to apply sufficient security, are also part of the privacy framework.

The national security community, on the other hand, focuses on collective existential harms, which, in politics jargon, have been securitized, and proposes punishment, reacting with indiscriminate surveillance.[248] Privacy and data protection cannot be seen as a complement to security, but simply as an obstacle to achieving control. The former must be balanced with the latter, in what is usually a zero sum game.

At the moment, there seem to be a shift of control from the technical community, to the more recent, institutional and national security-minded one, leading to the securitisation of the issue of cyber-security.[249] This is in line with the findings in section 2.4; cyber-security is increasingly referred to as a crucial national security issue, and the proposed measures either focus on deterrence or reaction. Nevertheless, it is necessary to cast a light on the term cyber-security. This usually refers to the policy

[246] Nissenbaum, "When Computer Security meets National Security," p. 59.

[247] Tien, "Architectural Regulation and the Future of Social Norms."

[248] Nissenbaum, 'When Computer Security meets National Security," p. 59.

[249] Ibid.

tackling the security of CII, whose specifications vary from country to country. In the US, which has an integrated and developed cyber-security policy,[250] the term refers to:

> "strategy, policy and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure."[251]

As illustrated in sub-section 2.3.2, information and communications infrastructures are CII, whose importance for (CIIP) is clear, due to the significance of CII for both government and private sector activities, and their cross-sector interconnectedness. From this definition it can be inferred that, in practice, CIIP translates into tackling online or narrow cybercrime as it relates to critical national services and government, and on a large scale. If this argument is true, the preventive practices for online cyber-crime should be the same as for CIIP. This is in line with the idea that cyber-security is an integrated and multi-layered system.

3.4.3 The OECD Guidelines

A good example is offered by the OECD Guidelines on Security, which set out the basis for building a culture of security. The guidelines are addressed to all 'participants' of information systems and networks, as each of them is deemed crucial to ensure security. In particular, nine principles are advanced, which must be considered as a whole, being intended as complementary.

The first and foremost principle is *awareness*, namely the acknowledgement of the need for security of information systems and networks, as well as knowledge of the tools needed to enhance security. Secondly, all participants should be *responsible* (*accountable*) for the security of information systems and networks, in proportion their roles. In particular, developers, designers, and suppliers of products and services are tasked with providing information and timely security updates. Thirdly, '*response'* to security incidents, which includes sharing information about threats and vulnerability, together with prevention and detection, should be handled timely and cooperatively. Fourthly, *ethics* should inform action, in that the pursuit of security should go hand in hand with the respect of the legitimate interests of those involved. Fifthly, the pursuit of security should also go hand in hand with the respect of the core values of *democracy*, such as: freedom of thought and expression, free flow of information, confidentiality of information and communications, the protection of personal information, openness and transparency. Sixthly, *risk assessments* of internal and external factors (technology, physical and human factor, policies and third-party implications) should be conducted by all participants. Seventhly, an essential element of information systems and networks should be *security*, incorporated throughout the *design*, *implementation* and co-ordination phases. For end-users this means choosing and configuring the appropriate services. Eighthly, a comprehensive and dynamic approach towards *security management* should be pursued, based on risk assessment and involving participants at all levels. It should include prevention, detection and response to incidents, systems recovery, on-going maintenance, review and audit. Finally, a continuous *reassessment* of threats and vulnerabilities, based on the results of the review, should lead to a change in policies, practices, measures and procedures.

---

[250] Porcedda, *Transatlantic Approaches to Cybersecurity*.

[251] The White House, *President's Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, 2009, p. 12.

The Guidelines are voluntary,[252] but their dissemination and adoption is encouraged. As seen in sub-section 2.3.2, the Council has recommended the adoption of these Guidelines as a model framework for the development of EU guidelines.

3.4.4 First hypothesis and first caveat on cybercrime and cyber-security

This section has hopefully contributed to demonstrate the theoretical validity of hypothesis one. Narrow or online cybercrimes, and broad or offline cybercrimes, are profoundly different in terms of underlying logics. The former essentially relates to data, while the latter incidentally relates to data, i.e. the data are a representation of a tangible situation in the offline world. I believe that computer-related and financial fraud fall in an intermediate category, but are closer to online cyber-crime, as the locus of activity is in the online world (i.e. e-banking), and they are usually a consequence of narrow cybercrimes. While the investigative and forensic techniques are the same, their impact is radically different, as online crime is affected by the problem of attribution. On the other hand, prevention seems of little use for broad cybercrimes, since the root of the crime is in the online world, whereas it is crucial to reduce the impact of narrow cybercrime at its root.

Only online or narrow cyber-crime pertains to cyber-security, understood as the policy tackling CIIP. Nevertheless, the current policy debate is focussing excessively on offline or broad cybercrime, whose techniques focus on reaction and surveillance, drawing attention away from what is needed most to tackle cyber-security:

> "policing the Internet, *as opposed to securing the computers that populate it*[253], may be a treacherous remedy. Will the government's monitoring tools be any more secure than the network they are trying to protect? If not, we run the risk that the surveillance facilities will be subverted or actually used against the [nation]. The security problems that plague the Internet may beset the computers that will do the policing as much as the computers being policed. If the government expands spying on the Internet without solving the underlying computer security problems, we are courting disaster."[254]

Moreover, architectural regulation acts as a *fait accompli*, in that it is usually covert or is not noticed by the average internet user, and affects the resources for action, making certain acts impossible, and therefore affecting the exercise of certain rights.[255] In other words, the design of the architecture can negatively affect the relationship between resources, social norms and rights. Building on this, for instance, the deployment of filtering as a default setting would act as a covert architectural regulation, undermining the social attitude of users towards privacy. CIIP and the prevention of narrow cybercrimes require exactly the opposite.

Caveat 1: in order to pursue CIIP, a stronger accent on prevention is needed, and therefore a prevalence of the technical approach, rather than the national security one. This in particular means raising all users' awareness, enhancing their responsibility to contribute to security. In a number of cases, this contributes to, and is increased by, the protection of privacy, whose caveats are going to be discussed in the next chapter.

---

[252] Presented in 1992, and reviewed in 1997 and in 2001, the Guidelines have been adopted as a Recommendation of the OECD Council on 25 July 2002.

[253] Italics mine.

[254] Withfiled Diffie and Susan Landau, "Internet Eavesdropping: A Brave New World of Wiretapping," *Scientific American Magazine* (September 2008), p. 4.

[255] Tien, "Architectural Regulation and the Future of Social Norms."

4. Data Protection and Privacy

4.1 Privacy and Data Protection: A Brief Introduction

It is well known that the concept of privacy originated long before the creation of computers; the seminal article by Brandeis and Warren[256] was published at the end of the 19th Century. The meaning of privacy has evolved over time, thanks to the inputs of crucial sentences and innovative legislation, to reflect the different needs of society, as widely described by the classic literature on the subject.[257] The diffusion of ICTs and especially computers has represented the greatest challenge to privacy, and the evolution of a neighbouring right, that of data protection (as an expression and evolution of informational privacy). The definition and scope of these rights vary according to the legal and social culture of each country, although there is agreement on a number of overarching principles, first expressed as Fair Information Practice Principles (FIPPs):[258]

> *i) collection limitation; ii) openness; iii) accuracy; iv) participation; v) security;*
>
> *vi) accountability; vii) purpose.*

The FIPPs have informed the basis of legal instruments such as the OECD Guidelines and the CoE Convention 108.

For the purposes of this discussion, the 'Security' principle, which reminds that data must be protected against possible theft and manipulation, is the most manifest link between privacy/data protection and cybercrime prevention, provided the word 'link' is appropriate to describe what are, in fact, two sides of the same coin. Openness and accountability, which result in transparency, are also crucial for this discussion. The former calls for informing citizens about existing policies; the latter suggests that the custodian of the data must be held accountable, for his or her deeds before existing rules. Citizens/users' awareness, as well as data custodians' accountability, are crucial in this area of overlap between privacy and cybercrime prevention. 'Citizens/users' and 'data custodians' become 'data subjects' and data 'controllers' in the EU legal translation of the FIPPs.

The EU boasts the most comprehensive data protection and privacy legal framework globally. On paper, it is certainly very advanced, but whether implementation keeps up with legal texts is another thing. Certainly, privacy is not an easy right to defend in an era when so-called free services are surreptitiously paid for through personal data, which has been indeed dubbed 'the currency' of our times; yet, this does not relieve the legislator from the responsibility of trying to provide the best possible rules.

I shall now turn my attention to the rules adopted by the EU, to show in more details how privacy and data protection can be integrated with cyber-security and cyber-crime prevention, which rests on two caveats: updating the legal framework, and adopting a core-periphery approach to privacy and data protection.

---

[256] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review*. Vol. IV, n° 6 (1890). Actually, in our times this article can be read with the lenses of data protection. Indeed, the event triggering it, namely the unauthorized diffusion of private photographs, pertains to the domain of personal data, pursuant to the definition of the Data Protection Directive.

[257] For some illustrations, see Chapter 1.

[258] Newman, *Protectors of Privacy*.

4.2 Privacy and Data Protection in the EU

The EU's data protection regime's outline has been deeply affected by the pillars structure, as two different regimes were established for the first and third pillars. The TEU and the TFEU contain several important innovations, which are likely to represent a major transformation in the privacy and data protection landscape. Nevertheless, until the legislative proposals advanced pursuant to the new provisions contained in the TFEU are executed, privacy and data protection will be governed by rules anachronistically based on pillars, and on an obsolete understanding of the relevant technology, as this section aims to prove.[259]

We can think of the data protection and privacy regimes as the sum of three levels of legal sources:

- International instruments, which impose obligations upon the EU as a whole or its MSs. These are in turn divided into:
    - Binding instruments: article 17 of the International Covenant on Civil and Political Rights; Article 8 ECHR, and the subsequent jurisprudence of the Strasbourg Court; the CoE Convention 108 and its Additional Protocol, whose detailed provisions apply to both first and third pillar; and the EUCFR;
    - Non-binding instruments and soft law: the 1980 OECD Guidelines; and the 1991 UN Guidelines;
- (Former) First pillar instruments:
    - The 'Data Protection' Directive 95/46/EC; Regulation 45/2001/EC;[260] and the 'E-privacy' Directive 58/2002/EC with its amendment.
- (Former) Third pillar instruments: the use of data by LEAs is an exception to the basic principles of privacy and data protection, which is regulated by three major groups of instruments:
    - "The Convention 108 with its Additional Protocol and the Recommendation 87 (15): as the first dedicated binding international instrument adopted (with the exception of the Recommendations), it established a benchmark for data protection in the former third pillar and still applies to the instruments entered into force prior to the adoption of Council Framework Decision 08/977/JHA;
    - Council Framework Decision 2008/977/JHA, whose scope is limited, in that it regulates the exchange of data between MS for all data exchanges which do not fall under a particular, or special, regime;[261]
    - Special regimes regulated *in leges speciales* such as those of Europol, [262] Eurojust,[263] Schengen[264] etc.,[265] whose benchmark is the Convention 108, its Additional Protocol and the Recommendation."[266]

---

[259] Porcedda, "Law Enforcement in the Clouds."

[260] Regulation 45/2001/EC, OJ L8, 12.1.2001, p. 1-21.

[261] In fact, although pursuant to article 1 the decision should also apply to "data exchanged between Member States and authorities or information systems established under the former title VI of the Treaty on European Union (TEU)" such as Europol/Eurojust, article 28 limits substantially this provision.

[262] Council Decision 2009/371/JHA, OJ L 121, 15.5.2009, p. 37–66.

[263] Council Decision 2009/426/JHA, OJ L 138, 4.6.2009, p. 14–32.

[264] Council Regulation (EU) 542/2010, OJ L 155, 22.6.2010, p. 23–26.

[265] European Commission, COM (2010) 385 final, "Overview of Information Management in the Area of Freedom, Security and Justice", Brussels, July 2010.

[266] Porcedda, "Law Enforcement in the Clouds," p. 221-222.

Pursuant to Declaration n° 21 to the Lisbon Treaty, these rules will be valid for at least an additional five years, unless amended or repealed. This is why a swift implementation of the innovations of the Lisbon Treaty is needed to dramatically simplify the current situation.

Firstly, the EU will be able to access the ECHR, therefore providing a direct connection between the ECJ and the European Court of Human Rights' (hereafter the ECtHR) case law. Very importantly, the EUCFR[267] has become binding and has acquired the same force as the Treaties – a constitutional-like force, in that its status is equalled with EU primary law and therefore has the same force. I shall elaborate on the significance of this innovation in the next section, as the EUCFR contains the germs for the adoption of a core-periphery approach to data protection and privacy.

Secondly, a new legal base for privacy and data protection has been introduced, namely article 16 TFEU[268] (and article 6 TEU),[269] which, following the abolishment of the pillars structure, applies to both former first and third pillars. The CFSP should be dominated by special rules, pursuant to article 39 TEU.[270] Article 16 envisages an obligation for the legislator to adopt rules pursuant to it and,[271] in fact, the Commission has proposed a new framework.

4.3 A Core-Periphery Approach of Data Protection and Privacy (Caveat 2)[272]

The new legal status of the EUCFR is crucial, because "it distinguishes between the right to private life (article 7) and to data protection (article 8), and provides a refined definition of the latter. In fact, articles 7 and 8 represent the latest definition of the right to respect for private and family life and data protection offered by previous instruments, namely article 8 of the ECHR, the CoE Convention 108, and the Data Protection Directive. Since these instruments follow a progression, they should be read and interpreted together. First, Convention 108 clearly refers to article 8 ECHR, both in the explanatory report to the Convention and in its Preamble "Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing. " The ECtHR has recalled this in several judgments.[273] It should also be pointed out that by means of this reference Convention 108 acquires a more ample purview than simply data protection. "…The very essence of the Convention is respect for human dignity and human freedom. Under Article 8 of the Convention in particular, where the notion of personal autonomy is an important principle underlying the interpretation of its guarantees, protection is given to the personal sphere of each individual, including the right to establish details of their identity as individual human beings."[274] As a result, a strong link is created between the right to private and family life and the right

---

[267] Although it does not create new rights, it offers a comprehensive collection of the fundamental rights protected under EU law. *The Treaty of Lisbon: An Impact Assessment. European Union Committee*, 10th Report of Session 2007-2008, 13 March 2008.

[268] TFEU, Art. 16.

[269] TEU, Art. 6.

[270] The problem of choosing the appropriate legal base between articles 16 and 39 may arise in the case of the external area of Freedom, Security and Justice. The hardest cases may need to be solved in court, without any treaty guidance. Marise Cremona, "The Two (or Three) Treaty Solution: The New Treaty Structure of the EU" in *European Union Law After the Treaty of Lisbon*, ed. Andrea Biondi et al. (Oxford: Oxford University Press 2012).

[271] Peter Hustinx (EDPS), "Data protection in the light of the Lisbon Treaty and the Consequences for Present Regulations", speech delivered at the 11th Conference on Data Protection and Data Security, Berlin, 8.06.2009; Hijmans, and Scirocco, "Shortcomings in EU Data Protection."

[272] This section, builds on, and innovates, previous work of mine in "Regulatory Challenges."

[273] For a detailed analysis of the ECtHR's case law, see Paul De Hert and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action," in *Reinventing Data Protection?* ed. Serge Gutwirth et al. (Springer, 2009).

[274] European Court of Human Rights. Case 28957/95: *Christine Goodwin v. United Kingdom*. Judgment, 11.7.2002, par. 90.

to data protection. Next, recitals (10) and (11) of Directive 95/46/EC also establish a strong relation vis-à-vis article 8 ECHR and Convention 108 respectively (thus confirming the strong link between the two rights). In detail "In detail, ―(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.‖ and ―(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data." […] Finally, since the EUCFR is the latest in a line, the same logic also applies to it: article 52.3 of the EUCFR reads "In so far as this EUCFR contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection." [275]

Therefore, article 7 and 8 build on, and enrich, previous definitions.

Article 7 lays down "everyone has the right to respect for his or her private and family life, home and communications." This article is substantially similar to article 8 ECHR, the only difference being the term 'communications' instead of 'correspondence', which reflects the ample purview of the term, in line with the jurisprudence developed by the Strasbourg and the Luxembourg Courts.

The real innovation is article 8, whose definition reads as follows:

> "1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data, which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority."

The new provision on data protection deserves some further discussion; in particular, it includes:

> "(a) Substantive principles on processing (which correspond to the substantive principles listed in article 6 of Directive 95/46/EC):
>
> 1. Fairness: to be fair, the processing must be 1) done for a legitimate purpose (legitimacy), which is defined either by the consent of the person (in the terms of article 6 of Directive 95/46/EC), or by law (i.e. article 7 of Directive 95/46/EC); 2) transparent, i.e. the data subject must be adequately informed (compare article 10 and 11 of the Directive);
>
> 2. Legality: all phases of the processing operations (including collection) must be carried out in accordance with the law, which must be clear, i.e. leaving no room for ambiguous interpretations, and foreseeable, i.e. the consequences of each provision must be known *ex ante* (lawfulness).
>
> 3. Purpose limitation: each processing operation must be tied to a specific, limited purpose (necessity and proportionality). The use of the same set of data for different purposes constitutes a new processing, subject to the conditions listed. The respect of purpose limitation is therefore crucial to an effective data protection regime.
>
> b) Procedural principles on processing:
>
> 4. Substantive rights: the data subject has the right of access to data concerning him or her, and to rectify them if they are not correct (compare with article 12 of Directive 95/46/EC);

[275] Porcedda, "Regulatory Challenges," p. 38-39.

> c) Control by an independent authority: no right is effective if it is not implemented and only the oversight of an independent authority can ensure compliance with these rules.
>
> Article 8 must be further read in conjunction with articles 51 and 52 of the EUCFR. The former limits the application of the EUCFR to Union law, while the latter recognizes that "subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others." Such interests are those listed in article 8.2 ECHR, or in article 9 of the Convention 108 or article 13 of Directive 95/46/EC, which include, among others, "(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; […] (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others." As a consequence […], data processing for police and judicial cooperation falls under the scope of the exceptions.[276] Nonetheless, the derogations listed must be provided for by legislative measures, and therefore have to respect the parameters established by the existing instruments.
>
> Furthermore, article 52.1 of the EUCFR reads as follows "any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms." The ECJ has made clear in several judgements that exceptions must be interpreted restrictively – as any exception; therefore (necessary and proportional pursuant to article 52 of the EUCFR), exceptions have to fulfil the essence of data protection,[277] as defined by article 8 of the EUCFR: legality, preciseness and foreseeability (lawfulness); fairness, legitimacy (consent, but not only) transparency; purpose limitation (proportionality and necessity); recognition of subjective rights; and independent supervision. Consequently, LEAs' practices should respect the substance of these principles without jeopardising investigations."[278]

It must be pointed out that the question of what constitutes the "essence" of data protection has not necessarily been closed by article 8. Further principles descend from other pieces of legislation. Indeed, the new legal framework contains innovative features, according to four pillars or principles as proposed by the EU Commissioner for Justice.

The first, which addresses privacy risks online, is the right to be forgotten, i.e. the actual withdrawing of consent to data processing, whereby "the burden of proof should be on data controllers."[279] The second one is transparency, which implies informing data subjects in a clear and straight-forward manner of the data collected, the purpose of the processing and the possible uses made by third parties, the risks involved in such processing, and to whom they should complain in case of a breach of their privacy. The third pillar is 'privacy by default', and relates to the idea that privacy should be the default option, instead of making it dependent upon changing cumbersome settings, which requires considerable operational effort.[280] The fourth pillar is protection regardless of data location: "any company operating in the EU market or any online product that is targeted at EU consumers must comply with EU rules." An overarching pillar, fundamental for effectiveness, is enforcement, leading to strengthening the independence and harmonising the powers of the EU DPAs.

Still, until a new instrument pursuant to article 16 TFEU is adopted, the most comprehensive definition of privacy and data protection will be the one offered by the EUCFR. Further research and discussions are needed to determine what principles constitute the essence.

---

[276] See, *inter alia*, Rodotà, *Elaboratori Elettronici*.

[277] For an excellent account of principles deriving from Convention 108, see De Busser, *Data Protection in EU and US Criminal Cooperation*.

[278] Porcedda, "Regulatory Challenges," p. 40-41.

[279] Vivianne Reading, "The Review of the EU Data Protection Framework," Brussels, 16 March 2011, SPEECH/11/183.

[280] For an early critique of consent, see Rodotà, S., *Elaboratori Elettronici*.

The objective of this section is to discuss the concept of the 'essence' of a right, which is similar to the result of a reinterpretation of Alexy's theory of right.[281] Accordingly, rights would have an inviolable core sealed in a rule, and a periphery subject to permissible limitations, such as those foreseen by article 8 ECHR, and articles 7 and 8 of the EUCFR, for privacy and data protection. This core-periphery approach to rights lays the basis for an integration of the compliance with the rights to privacy and data protection and the needs of LEAs when conducting an investigation and, in a more general fashion, privacy and security, as opposed to the theories of balancing.[282]

The core-periphery approach, in fact, can lead to building better rules on data protection as a layered structure, meaning that the same principle could be addressed in different ways according to the circumstances. For instance, the principles of access and rectification presuppose notification of processing. Nonetheless, during an investigation, it is not conceivable to inform the data subject of the processing beforehand without jeopardising the operation. Yet, the simple matter of the existence of an investigation does not justify the complete encroachment of the principle of access and rectification. Therefore, in case of an investigation, the DPAs could be notified instead, and control the correctness of the data (at the moment, DPAs can access the data held by LEAs on behalf of citizens, but are not notified). As soon as the data collection exercise ceases needing to remain secret – i.e. the evidence has been obtained – the data subject can then be informed and exercise his/her rights in full. The same exercise may be repeated for each principle constituting the core (whose specification is outside of the scope of this research). A similar mechanism may be envisaged for the independent control in general.

This is important in general, and for cybercrime and cyber-security in particular, for two reasons. First of all, investigations on cybercrime, whether narrow or broad, will happen and, in that case, privacy and data protection will be perceived as values competing against others, in a situation which "may require diminishing the satisfaction of some values in order to advance the satisfaction of other values", with the objective of achieving "the best overall outcome, i.e., balanced maximisation."[283] For narrow cybercrime in particular, there could be a clash between the preventive and the reactive phase.

In theory, through a core-periphery approach, rights can be built (i.e. laws can be devised) in such a way as to include 'by design' the exceptions, to limit piecemeal, *ad hoc* solutions; this could avoid the need for balancing in the case of broad cybercrime, and of any other crime. Theoretically, a direct channel could be created between LEAs and DPAs, with a view to building a co-operative relationship in the case of investigations, similar to the cooperation started by the WP29 and ENISA, which would be particularly fruitful in the case of cybercrime. Whether this is feasible, though, has to be demonstrated by further research.

4.4 Updating the Data Protection Provisions: The Test of Cloud Computing (Caveat 3)[284]

At the beginning of this year, the Commission has proposed two new instruments pursuant to article 16, namely a 'Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data', and 'Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data'. Both instruments build on the Commissions' Communication 'A comprehensive approach on personal data protection in the EU,

[281] Scheinin, "Terrorism and the Pull of 'Balancing' in the Name of Security."

[282] Sartor, "Doing Justice to Rights and Values."

[283] Ibid.

[284] This section, builds on, and innovates, previous work of mine, in "Regulatory Challenges" and "Law Enforcement in the Clouds."

COM (2010) 609 final' and implement its rationale.[285] Notwithstanding the soundness of the main objectives of the Data Protection Directive, i.e. the protection of fundamental rights and the pursuit of the internal market, the Communication acknowledges that the regime needs some corrections, not only because of the institutional change realised by the Lisbon Treaty, but also due to more structural problems.[286]

For instance, DPAs play too marginal a role. Multinational businesses across the EU have lamented the legal uncertainty and unfair competition resulting from the current level of harmonisation. In spite of the existence of tools such as PETs to counter the increased risks, and the increasing recognition of their importance, little action is being taken to turn assertions into practice, and therefore reduce risks.[287] New technologies, in particular, test data protection. Data collection has grown in sophistication and surreptitiousness, resulting in a loss of control of one's own data, as in the case of "Internet-based computing whereby software, shared resources and information are on remote servers ('in the cloud'),"[288] i.e. cloud computing. Cloud computing is particularly relevant, because it is regarded as the future of computing (especially in connection with the phenomenon of big data). The new data protection regime must therefore be 'cloud computing proof'.

The next step is, therefore, to build on existing analysis of the impact of cloud computing, to appraise the specific proposals advanced. It is understood that cloud computing is not the only challenge to data protection and privacy and, therefore, a more comprehensive analysis of the new proposal is needed. I shall give a brief description of cloud computing, before appraising the Commission's proposed changes – as resulting from a combination of COM (2010) 609 final and the proposed Regulation – against the challenges they bring about.

4.4.1 A brief description of cloud computing

First of all, cloud computing is not a new technology. The virtualisation of computing resources it entails, meaning the disconnection between hardware and software, allowing one single CPU (Central processing unit) to run several operating systems at the same time, thus giving the impression that several computers are available, was already realised in the 1960s by IBM.[289] Simply, for some decades the trend in computing was the opposite, as the decrease in prices allowed everybody to afford a personal computer. Virtualisation was restored as an emerging effect of the business practices of firms such as Microsoft, Google and Amazon, as a technology allowing a reduction in the management costs of handling all the switches in computing resources to run services such as Hotmail and Messenger in the case of Microsoft.[290] Only after these firms realised the potential of capitalising on virtualisation did the cloud become a business model, and has now 'conquered' the hearts and minds of individual users, businesses of all sizes, and governments, for its ability to increase the efficiency of their IT infrastructure while cutting costs.

Much like cybercrime, cloud computing is a blurred concept: "cloud computing has been talked about, blogged about, written about…Nevertheless, confusion remains about exactly what it is and when it is

---

[285] European Commission, "A Comprehensive Approach on Personal Data Protection in the European Union." COM (2010) 609 final.

[286] Article 29 Working Party and the Working Party on Police and Justice, *'The Future of Privacy': Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data*, (WP 168), December 2009.

[287] "Overall, many of the representative bodies with a remit that incorporates PETs are convinced of the need for PETs, but benefits are often asserted rather than demonstrated with evidence." COM (2010) 609, p. 14.

[288] Ibid., p. 2.

[289] OECD, Conference "Cloud Computing: Concept, Policy Implications, and Future Trends," 10 October 2011.

[290] Ibid.

useful…"[291] 'The cloud' means different things for providers, users and states. The first ones consider it as a 'competitive proposition', the second ones as a pay-as-you-go and dynamic utility, and the third ones as eco-systems for innovation. Although several definitions exist, I prefer to recall all accepted characteristics, instead of pitting one definition against the others.[292]

Cloud computing rests on the so-called datacentres (or data farms), and clusters[293]: aggregations of powerful servers where data are stored. Datacentres are built in those countries offering the most advantageous conditions in terms of taxes, electricity and cooling costs, and are often dispersed among different countries (and therefore jurisdictions). Since datacentres require investments in the order of US $billions, only a few companies - notably Amazon, Google, Microsoft and a few others- can afford such levels of investment. As a result, other companies wishing to offer cloud products rent, i.e. outsource, resources from these vendors; outsourcing can also take place for some of the services they offer. Outsourcing and the presence among multiple jurisdictions exacerbate the consequences of two characteristics, namely scalability and elasticity (dynamicity).

Cloud computing is scalable, meaning that it can be offered to a potentially unlimited number of customers. It is also dynamic, or elastic: the resources are provided in higher or lesser amounts according to the customers' needs. Such resources can come from different data centres, depending on the number of services requested, so as to offer a seamless service. This has two consequences.

The first one feeds on the system: an ever increasing amount of computing capacity is needed to avoid service failure – which gives the impression of infinite resources – and reduces the costs of renting computing capacity, thus making the cloud more attractive to customers and service developers. The second one is that the data, and eventually the bits, which are the building block of the service, are constantly moved around the datacentres: at any time, the users (and probably also the outsourcers) are not able to say where one's data is. Nor do they have to ask, as this whole process is hidden from their view: to them, the service appears seamless.[294]

Another consequence is that cloud computing tends to be multi-tenant: different entities (whether firms or people) can subscribe to the same services and use them contemporaneously. Multiple-use is possible thanks to an 'insularisation' of the computing resources and storage capacity allocated to each customer, and the use of appropriate programs allowing the distribution of the same product to different subscribers at the same time. Multi-tenancy is also referred to as public cloud, as opposed to private clouds, which entails dedicated, often resident, datacentres, usually demanded to store confidential information. The advantage of private clouds, beyond the control of one's data, is the ability to exercise more power vis-à-vis the provider, and possibly negotiate the terms and conditions of use, as opposed to public clouds' customers which can only agree to a pre-packaged solution (not necessarily advantageous to them). While one may ask whether resident data centres constitute clouds, one should note that a private solution overturns the advantages of the proper cloud. Indeed, the alternative has been to offer hybrid clouds, whereby the bulk of confidential information can be kept under control by the customer, whole non-sensitive activities can be carried out through a public cloud, and consumed according to need.

---

[291] Michael Armbrust et al., "Above the Clouds: A Berkeley View of Cloud Computing," Technical Report No. UCB/EECS-2009-28, February 10, 2009, p. 3.

[292] Kenji E. Kushida et al. "Diffusing the Fog: Cloud Computing and Implications for Public Policy" BRIE Working Paper 197 March 11, 2011.

[293] "The clusters offer the execution of programs with a high level of speed." Gayrel et al. "Cloud Computing."; Porcedda, "Regulatory Challenges."

[294] Furthermore, "an organization may not know where the data they are responsible for is located geographically at a particular time, although this may be more of a logical structure, than a geographic one." (Mark Taylor et al. "Digital Evidence in Cloud Computing Systems", *Computer Law and Security Review* 26 n° 3 (2010): 304-308).

The type of services offered by the cloud are usually classified as 'infrastructure as a service (IaaS)', 'platform as a service' (PaaS) and 'software as a service' (SaaS). Iaas refers to the actual infrastructure, or hardware, i.e. computing resources and storage capacity. The PaaS refers to a virtual operating system, which allows users to deploy it for their ends, without having to manage the underlying infrastructure (i.e. Microsoft Azure or Google Android).

SaaS encompass the services and contents most widely known to the public: from web-based email, through to data storage services and instant messaging/social services, to online streaming services. While users are lifted from the burden of administering the supporting programs (for instance, keeping them updated), they lose material control of the data. In turn, this raises the question of who possesses the data. These services usually – but not always – target different audiences. SaaS encompass the services mostly known to the general public, whereas PaaS and IaaS are generally directed at businesses and enterprises. It should also be noted that subscribers and end users do not necessarily coincide (i.e. there can be one subscriber and several users).

Since the cloud would not exist without the Internet, and its diffusion depends on the skyrocketing availability of devices allowing to be connected round-the-clock, the cloud environment involves also Internet Access Service Providers and access devices providers. A turf war seems to have emerged between these three actors, with the IASPs losing out, and the cloud provider winning. While the former's expansion to other services is strictly limited by regulation, the latter are not hindered by such limitations and can therefore develop in the other field.[295] Google is supposed to possess the third-most developed network in the world.

While these last remarks drift from the main discussion, they show that, whatever definition of the cloud is chosen, its appeal is bound to rise, and probably spark unforeseeable developments and regulation.[296] I can now analyse how the cloud interacts with data protection and privacy legislation, and evaluate the Commission's proposals, i.e. COM(2010) 609 and the proposed Regulation.

4.4.2 The definition of personal data

"The definition of personal data laid down by article 2(a) of Directive 95/46/EC marks the division between data deserving protection or not. As unpacked by the WP29,[297] the definition excludes, inter alia, data relating to legal persons and know-how,"[298] unless falling under the restricted cases of Directive 2002/58/EC (which explicitly mentions the legitimate interest of the subscribers who are legal persons, as regards articles 12 and 13 on unsolicited communications). This would be the case for the many enterprises and businesses using platform and infrastructure as a service. In principle, protection under the Directive can be extended to legal persons, and the ECtHR has recognised the protection of one sphere of privacy to legal persons;[299] however, only Italy,[300] Austria and Luxembourg have indeed extended some of the provisions of the Directive to these subjects.

Additional exceptions are to be found in article 2(c) on unstructured data, and in article 3(2) on data processed for domestic purposes. The latter is controversial, and particularly relevant for cloud-based services. In fact, while many popular cloud services such as social networks and web-based emails fall

---

[295] The EU Security Roundtable, *European Cyber Security Conference Shared Threats – Shared Solution*s.

[296] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing," Version 15, July 10, 2009, available at: <http://csrc.nist.gov/groups/SNS/cloud-computing/>.

[297] Article 29 Data Protection Working Party, *Opinion N. 4/2007 on the Concept of Personal Data* (WP 136), June 2007.

[298] Porcedda, "Law Enforcement in the Clouds," p. 211.

[299] Mario Viola de Azevedo Cunha, "The Concept of Personal Data in the Post Lisbon era: is there need (and room) for change? In *Data Protection in Good Health? Ed.* Serge Gutwirth et a. (Springer, 2012).

[300] Legislation recently enacted, though, has substantially reduced the extent to which legal persons fall within the scope of the Decreto Legislativo n.196 of 2003, which transposed Directive 95/46/EC into Italian law.

under the household exception's umbrella, the Lindqvist case and the WP29 interpretation made clear that the Directive would apply when data are made available to a large public;[301] in practice, though, this will probably be addressed on a case-by-case basis.

COM (2010) 609 recognised that the broad and flexible approach allowed by the concept of personal data, and the processing permitted by certain technologies, often meant that "there are numerous cases where it is not always clear, when implementing the Directive, which approach to take, whether individuals enjoy data protection rights and whether data controllers should comply with the obligations imposed by the Directive." The Commission then recognised that the definition of sensitive data should have encompassed new categories deserving protection, as indeed laid down by article 4 of the proposed Regulation (i.e. biometric and genetic data). However, the proposed Regulation does not protect legal persons' data, as personal data are information relating to a data subject, i.e. a natural person (article 2(a) and (b)). This is unfortunate, "since problems concerning the processing of…data can affect both legal and natural persons,"[302] with the exception of physical, physiological and mental data. Actually, pursuant to Directive 95/46/EC data protection rules can be extended to legal persons by the data controller, in order not to apply two standards to the same processing. Therefore, if legal persons were affected by cybercrime, they could enjoy additional protection. Hence, the inclusion of data on legal persons in the new text would contribute to making data protection rules complementary to cybercrime rules.

As for the household exception, article 2 of the proposed Regulation refer to processing done "without any gainful interest in the course of exclusively personal or household activity." The wording chosen is unlikely to solve all ambiguities connected to this exception.

4.4.3 Data controller and data processor

As put by the EDPS, "Internet users act as data controllers ex article 2(d) of the Directive for the data that they upload. However, in most cases [social networking] processing falls within the household exception ex article 3(2) of the Directive. At the same time, special networking services are considered data controllers insofar as they provide the means for processing user data and provide all the basic services related to user management (e.g. registration and deletion of accounts)."[303] Indeed, cloud computing weakens the distinction between controllers and processors.[304] "According to both the Directive and many cloud computing privacy policies, the controller would be the user, who in many cases lacks the technical competence and knowledge (the control of the means and purposes) to act as such. In fact, forms of co-control may exist *de facto*. This complicates the attribution of responsibility,"[305] as well as the availability of protection to citizens. "The definition of 'data controller' and 'data processor', i.e. the 'inner circle of data processing', is very important, as it allocates responsibilities for effective application of and compliance with data protection rules.[306] Inter alia, the controller offers an essential criterion when choosing what is the applicable law (article 4) and s/he ensures the enforceability of data protection rights, both proactively (ensuring implementation) and reactively (ensuring compensation). […] The controller is also in charge of notifying access to data by LEAs, notification of security breaches, and responsibility for security and liability. The identification of the data processor is highly relevant, too, in order to ensure the confidentiality and

---

[301] Ronald Leenes, 'Who Controls the Cloud?,' *Revista de Internet, Derecho y Politica*,n° 11 (2010).

[302] De Azevedo Cunha, "The Concept of Personal Data," p. 28.

[303] EDPS, *Opinion on Privacy By Design*, March 2010, p. 14.

[304] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of 'controller' and 'processor'* (WP 169), February 2010.

[305] Porcedda, "Law Enforcement in the Clouds," p. 212.

[306] Peter Hustinx (EDPS), "Data Protection and Cloud Computing under EU law" (speech delivered at the Third European Cyber Security Awareness Day, Brussels, April 2010); Gayrel et al. "Cloud Computing."

security of processing (articles 16-17), and the applicable law for security of processing, which depends on whether or not the processor is established in the EU.[307]„[308]

The situation is further complicated by the phenomenon of cloud outsourcings, mergers, and by the sale or transfer of data for profit. "Indeed, especially because of this grey zone, cloud computing providers may be using users' data for profitable meta-processing activities."[309]

Such legal vacuum brings about insufficient compliance with data protection laws, and generates unequal powers between individuals and corporations, and between corporations themselves. The new Chapter IV of the proposed Regulation tackles the legal vacuum, in that it envisages forms of joint control (articles 24 and 26), thus partially addressing the problem of the exact attribution of the quality of 'controller' (the proposed definition does not seem to provide help in this respect), and the problems of outsourcing and data sales.

As for the imbalance of powers, the WP29 suggested introducing persuasive sanctions and the principle of accountability.[310] The principle requires adopting policies and taking appropriate measures to implement data protection principles (also when transferring data abroad), and being able to demonstrate that such appropriate and effective measures have been taken (evidence). This could be done by means of monitoring or conducting internal/external audits. It follows that transparency is an integral element of accountability.

COM (2010) 609 envisaged the application of both principles. Article 22 of the proposed Regulation puts into effect the principle of accountability as described above. This provision should be read in conjunction with the new provisions on the principle of transparency and on consent, which are analysed in section 4.4.3 below. The Communication's additional suggestion to oblige controllers to appoint a data protection officer, following the examples of Germany and France, is laid down in article 35. Whereas the appointment of a DPO is subject to specific provisions, cloud computing seem to fall within the scope of article 35(c), since the provision of cloud computing services requires the "regular and systematic monitoring of data subjects". This will hopefully ensure the correct application of data protection rules and offer assistance to individuals. The Commission further proposed to introduce mechanisms to ensure compliance with data protection rules, such as promoting the use of PETs,[311] and Privacy by Design (PbD), which are discussed more extensively below.

4.4.4 Applicable law and data transfers

From a data protection standpoint, "in many circumstances the use of cloud computing services will entail international data transfers. This calls into question the validity of the concept of adequacy, the helpfulness of the existing rules on data transfers and on applicable law, as well as the enforceability of data protection and privacy rights."[312] The issue can be better addressed by dividing cloud services into two categories (from an EU perspective): mono-jurisdictional and trans-jurisdictional clouds.[313]

---

[307] Article 29 Data Protection Working Party, (WP 169).

[308] Porcedda, "Law Enforcement in the Clouds," p.211-212.

[309] Ibid., p. 213.

[310] Article 29 Data Protection Working Party, "Opinion 3/2010 on the Principle of Accountability" (WP 173), July 2010.

[311] European Commission, *Promoting Data Protection by Privacy Enhancing Technology (PETs)*, COM (2007) 228).

[312] Porcedda, "Law Enforcement in the Clouds," p. 214.

[313] Roger Clarke and Dan Stavensson, "Privacy and Consumers Risks in Cloud Computing", *Computer Law and Security Review* 26 n°4 (2010), 391-397. Porcedda, "Law Enforcement in the Clouds."

In the EU, a cloud is "**mono-jurisdictional** if the conditions laid down by article 4 of Directive 95/46/EC are satisfied: either the controller is located within the EU or, it uses equipment located in the EU for purposes other than those of transit."[314]

The first case is not as simple as it may appear because, even if the jurisdiction is the same, the market is fragmented due to the fact that MSs enacted different e-laws. COM (2010) 609, in line with previous policy documents,[315] recognised that the room of manoeuvre allowed in the implementation of the Directive had resulted in additional costs and administrative burdens for the economic operators. As a result, the goal of ensuring the free flow of personal data within the internal market had been hindered, and uncertainty for data subjects created. The new instruments is a Regulation exactly to favour the highest level of harmonization; the same rationale applies to the concept of the 'main establishment' introduced by article 4(13), i.e. the place where the controller takes the "main decisions as to the purposes, conditions, and means of the processing of personal data" or, if the controller is outside the EU, "where the main processing activities…take place," and the place where the controller has its central administration. The main establishment is relevant to allocate competence to a Supervisory Authority in the context of a dispute, when the controller is established in several MSs. With a view to increasing legal certainty and providing a level playing field for data controllers, COM (2010) 609 suggested a review of the notification system, which is laid down by article 28 of the proposed Regulation.

As for when the second case, "the 'equipment' criterion is also likely to raise important issues because of the characteristics of cloud computing. Not only laptops, but cookies can be considered equipment,"[316] as the WP29 has established. In many cases, cloud computing services would save cookies on the users' devices, both to facilitate service use, and to permit behavioural advertising. Directive 95/46/EC should apply to this type of cloud computing services, unless the user has preventively blocked them.[317] The WP29 had already advocated a revision of the rules on applicable law.[318]

The Commission recognised the need to clarify the rules on applicable law and MSs' responsibility, explicitly because of globalisation and technologies such as cloud computing, which challenge the implementation of applicable law, thus depriving data subjects of their rights. Indeed, article 3 of the proposed Regulation widens the scope of application, and replaces the 'equipment' clause with two other caveats. The Regulation applies when processing relates to 'the offering of good and services to data subjects in the Union' and 'the monitoring of their behaviour.' This will apply to most cloud computing services.

"Although domestic clouds are desirable from a policy[319] perspective, they are accompanied by the existence of **trans-jurisdictional clouds**, which encompass both proper multinational actors (i.e. Amazon, Google, Microsoft etc.), which are therefore faced with the legislation of several jurisdictions, and clouds based under one jurisdiction only but operating through several data centres in the world," which are not based in the EU. […] "While the place of the establishment should not

[314] Porcedda, "Law Enforcement in the Clouds," p. 214.

[315] European Commission, *A Digital Agenda for Europe*; ENISA, *Cloud Computing, Benefits, Risks*.

[316] Porcedda, "Law Enforcement in the Clouds," p. 214.

[317] See Leenes, "Who Controls the Cloud?"

[318] Article 29 Data Protection Working Party, (WP 168).

[319] However, computer scientists maintain that domestic clouds would significantly reduce the convenience of cloud computing services, which benefit from the dispersal of data centres around the world (and therefore among different jurisdictions).

matter from the standpoint of article 4 of Directive 95/46/EC,[320] it may further complicate the problem of the applicable law in practice."[321]

The point about trans-jurisdictional clouds is that they are based on incessant data transfers outside the EU, and therefore trigger the application of the relevant articles of Directive 95/46/EC. The data can be transmitted either if the receiver ensures an adequate level of protection (art. 25), or if one of the exceptions pursuant to article 26 applies, such as the use of binding corporate rules, exceptions that must be interpreted restrictively.[322] These rules, though, are based on an old conception of point-to point', contract-based transfer.[323]

While COM (2010) 609 regarded binding corporate rules as a good answer, besides more extensive intervention, it recognised the insufficiency of the parameters laid down by articles 25 and 26. Therefore, it intended to clarify and simplify the rules for international data transfers. In addition, since articles 25 and 26 ignore non-contractual situations, data transfers between public administrations are not covered/cannot take place accordingly, and MSs end up using different rules to assess third states' level of protection; the proliferation of international agreements may also entail different standards for different instruments.

Indeed, data sharing (including that related to law enforcement) with third countries that do not offer an adequate level of protection, is becoming more common,[324] and this is especially true, although implicit, in the case of cloud computing. Threats increase and acquire a stronger international character. Therefore, in order to both prevent threats and protect its citizens, the EU tries to export its principles, specifically by means of agreements and by leading negotiations on international standards.[325] In line with this ambition, COM(2010) 609 intended to:

> "continue to promote the development of high legal and technical standards of data protection in third countries and at the international level; strive for the principle of reciprocity of protection in the international actions of the Union and in particular regarding the data subjects whose data are exported from the EU to third countries; enhance its cooperation, to this end, with third countries and international organisations, such as the OECD, the CoE, the UN and other regional organisations; closely follow up the development of international technical standards by standardisation organisations such as CEN and ISO, to ensure that they usefully complement the legal rules and to ensure operational and effective implementation of the key data protection requirements."[326]

Article 45 of the proposed Regulation translates this programmatic statement into rules for establishing international cooperation with a view to protecting personal data. More in general, Chapter V of the proposed Regulation addresses the issue of transfers to third countries and, as an innovation, to international organization. Article 41 adds new burdens to issue decisions of adequacy. Besides adequacy decisions, transfers will be allowed, pursuant to article 42, by means of binding corporate rules (further regulated by article 43), standard data protection clauses adopted by the Commission or a Supervisory authority, contractual clauses, and authorization from the supervisor.

---

[320] Leenes, "Who controls the Cloud?"

[321] Porcedda, "Law Enforcement in the Clouds," p. 216. Clarke and Stavensson, "Privacy and Consumers Risks in Cloud Computing."

[322] Porcedda, "Law Enforcement in the Clouds," p. 215. Article 29 Data Protection Working Party, *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (WP 12), July 1998.

[323] Hustinx, "Data Protection and Cloud Computing."

[324] See, inter alia, the implementing rules of the Council Decision 2009/371/JHA, available at: <http://www.europol.europa.eu/index.asp?page=legal_other>.

[325] Ibid.

[326] COM (2010) 517 final, p. 17.

4.4.5 Consent in the cloud and terms of use

Despite the unlawfulness of processing data without the informed and free consent of the data subject, the use of unadvertised cookies, the practice of behavioural advertising, and the phenomenon of purpose creep (the three often being intertwined), are common practice. Alas, consent in the cloud –as in other domains – appears a chimera principle.[327] Users' unawareness, and the often unclear and vexatious terms of service, contributes towards this state of being.

COM (2010) 609 recognised that the meaning of, and rules relating to, consent are not clear. The WP29 recommended clarifying in particular the terms 'unambiguous', to put in place a mechanism that forces controllers to demonstrate consent, as well as to ensure the quality and accessibility of the information, and to address the situation of minors and those not having legal capacity.[328] Article 7 of the proposed Regulation introduces new rules on consent, whereby the controller "bears the burden of proof for the data subject's consent", which has to be given for each specific purpose carried out by the controller.

Furthermore, appropriate and accessible information is of the utmost importance, as it is at the base of consent. Following the acknowledgment of the results of a Eurobarometer survey, according to which privacy awareness perception is low among the public, COM (2010) 609 proposed to raise awareness, by co-financing dedicated activities, or rendering them mandatory. The point is especially welcome, because of the surreptitious character of the data collection online, and the users' little awareness of the privacy (and security) risks entailed.

The state of the art may be worsened by the terms and conditions proposed by cloud computing providers; "on most occasions the user does not have any negotiation power and must accept the policies as they are. These often include: limited (if any) liability for the integrity of the data; disrespect of the confidentiality of content; disclaimers against guaranteed provision/continuity of the service; imposed applicable law; and difficult data recovery after termination of services. In addition, providers engage in different levels of obligation to notify users of data disclosure, typically to LEAs.[329]"As for the latter, the American providers, which offer some of the most popular cloud services, are all subject to the Patriot Act; I will return to this point later in this section.

COM (2010) 609 establishes "the requirements that the information must be easily accessible and easy to understand, and that clear and plain language is used,"[330] which does not seem to be happening in the online environment, as shown by the Eurobarometer survey. The Communication recognises that this is detrimental to the understanding of behavioural advertising and the use of the Internet by children. The Commission therefore proposed to reform articles 10 and 11 of the Directive, as well as to include a new principle on transparent processing; new obligations for data controllers on the type of information; and modalities to provide and the adoption of EU standard forms on privacy information notices.

Indeed, the proposed Regulation puts into effect the principle of transparency, laid down by articles 5(a) and 11. The latter and mandates the use of "easily accessible policies" and the provision of communication written "in intelligible form, using clear plain language." article 14 further specifies the elements that must be contained in an information notice. As for the protection of particularly vulnerable data subjects such as children, article 8 lays down new rules on consent for children below the age of 13, which should be provided by the parents or custodians.

---

[327] Rodotà, *Ëlaboratori Elettronici*.

[328] Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent*, (WP 187), 13 July 2011.

[329] Simon Bradshaw, "Cloud Computing: Security and Privacy Aspects of Cloud Contracts" (Conference presentation, Ankara, May 2010); Simon Bradshaw et al. "Contracts for Clouds: A Comparative Analysis of Terms and Conditions for Cloud Computing Services" (Queen Mary School of Law Legal Studies Research Paper No. 63/201, London, 2010).

[330] European Commission, COM (2010) 517 final, p. 6.

Finally, COM (2010) 609 proposed to strengthen the existing rules on sanctions, study the feasibility for DPAs and (civil society) associations to bring an action before the national courts and, as a future action, pursue an active infringement policy. The combination of chapter III on the rights of the data subject and chapter VIII on liability and sanctions of the proposed regulation give substance to these intentions. In particular, article 79 confers powers on DPAs to issue administrative sanctions which are "effective proportionate and dissuasive." Such sanctions should amount to up to 250 000€ or 0,5% of its annual worldwide turnover, for those enterprises breaching articles 12(1), (2), and (4), namely for not providing mechanisms for requests by data subjects, providing them wrongly, not answering, or charging a fee to address the request, as set up by article 79(4). In case of violation of the provisions relating to the rights of the data subjects provided for in chapter III, article 79 (5) lays down that the fine will be up to 500 000 or 1% of the annual worldwide turnover. Finally, the sanction can be up to 1 000 000 or % of the annual worldwide turnover, as laid down by article 79(6), when data are processed, *inter alia*, (a) without sufficient legal basi and consent pursuant to articles 6, 7 and 8; (b) special categories of data disrespecting articles 9 and 81, (d) or conditions for carrying out profiling pursuant to article 20.

Finally, article 73(2) of the proposed Regulation allows civil societies associations to lodge a complaint with a supervisory authority on behalf of one or more data subjects whose rights have been breached.

4.4.6 Data security principle

Data security is a one of the fair information practices principles (FIPPs) and, consequently, a core principle of data protection. It "implies two factors, namely organizational and technical measures, appropriate to the risks posed by the processing activity, provided these are technically and economically feasible for the controller or the processor- if different- which must in turn be chosen in an accurate manner."[331] The obligation to take the appropriate security measures follows the data in every new processing, and applies to any controller or processor, including service providers (when they do not qualify as controllers[332]) and LEAs, as provided for by recital 30, articles 10 and 22 of the Council Framework Decision 2008/977/JHA and article 7 of the Data Retention Directive.

Security of the data in the cloud is debated. While using the cloud allows one to shield oneself from one's own system's failure, new problems arise, beyond the limits posed to security and confidentiality by the terms of service. First of all, because clouds store massive amounts of data, they become more attractive to cyber-criminals. The point is of course crucial for this research. Examples of 'data breaches' abound.[333] In the event of a clouds' failure, all users' data are lost. "Since it is difficult to understand what is in a cloud from the outside, users should refrain to think about clouds as big and secured services."[334] Observing the appropriate level of data security in respect to the possible risks would considerably curtail the risk of threats to computer data and infrastructure, an d narrow cybercrime in general.

The current trend in data security is PbD,[335] which "refers to the philosophy and approach of embedding privacy into the design specifications of various technologies. This may be achieved by building the principles of Fair Information Practices (FIPs) into the design, operation and management

---

[331] Porcedda, "Law Enforcement in the Clouds." P. 219.

[332] Article 29 Data Protection Working Party, (WP 168).

[333] See, for instance, at http://datalossdb.org/statistics. One of the most recent ones is the double hack into Sony's players' servers.

[334] Bradshaw, "Cloud Computing."

[335] See Article 29 Data Protection Working Party, (WP 168); EDPS, "Opinion on Privacy by Design."; European Commission, *A Digital Agenda for Europe*.

of information processing technologies and systems. [...] In total, the three areas of application are: (1) technology; (2) business practices; and (3) physical design."[336] PbD is rarely put into effect in these three domains, because of a lack of incentives, as described in previous sections, and lack of market demand, usually due the abovementioned lack of awareness of users. As for the current legislation, article 14.3 of the e-Privacy Directive lays down rules on PbD, in that "where required, measures may adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data." The EDPS, though, noted that this provision has not been implemented, which suggests that in order to step up security in cloud services, [337] action is needed as much as rules setting up the right incentives.

An attempt to put forward the necessary regulatory incentives is the introduction of the notification of data disclosure and security breaches. This is a global, albeit slow, trend. In the US, data breaches notification, which is mostly seen as a consumer protection issue under the control of the Federal Trade Commission, is mandatory for banks at the federal level, and mandatory data breaches notification laws have been applied in most of the States. Several DPAs are starting to monitor the breaches and, in the absence of pertinent laws, have introduced guidelines for voluntary notification. In the EU, the reviewed e-Privacy Directive has introduced mandatory notification of security breaches, but only for providers of public electronic communications services, as recalled in Chapter 2.

Through COM (2010) 609, the Commission announced that it would initiate preparatory works on extended data breaches notification by the end of 2011. The WP29 applauded this intention, and recommended undertaking the harmonization of the framework as soon as possible.[338] In addition, the Commission explicitly proposed implementing PbD, as well as introducing privacy seals, as a further contribution to better implementing data protection rules. It recognised that enforcement depends on the powers attributed to the dedicated institutions, and therefore called for a strengthening of the role of DPAs, and an increased coordination of their activities, and as a consequence an improvement of the WP29.

The proposed Regulation favourably translates the plan of the Communication into provisions. Article 23 introduces the principles of data protection by design and by default. Section 2 of chapter IV includes two provisions on the obligation to notify data breaches, and envisages security obligations both for controllers and processors. Article 33 introduces data protection impact assessments, and article 39 proposes the use of certification and seals. Article 79(6) on mandates the harshest administrative sanctions for violations concerning infringements of data security provisions, as well as data security breaches.

As for enforcement, article 64 of the proposed Regulation introduces the Data Protection Board, which should replace the WP29, and article 53 provides equal and increased powers to all DPAs, or Supervisory Authorities, including investigative powers to access information and premises. These authorities should cooperate with each other and the Commission, provided that, in case of controllers or processors established in more than one member state, the supervisory authority of the main establishment of the controller or processor is competent.

This is also very relevant in case of an investigation involving data in the clouds. The cloud environment challenges the current forensic techniques in computing.[339] Technical and procedural data

---

[336] Cavoukian, *Privacy by Design*.

[337] EDPS, *Opinion on Privacy by Design*, par. 34.

[338] Article 29 Data Protection Working Party, *Working Document 01/2011 on the Current EU Personal Data Breach Framework and Recommendations for Future Policy Developments.* (WP 184), 5 April 2011.

[339] Challenges vary in case the data are stored in a public or in a private cloud. Extraction of the data seems easier in the private cloud, for it tends to be a circumscribed ecosystem, as opposed to the dynamic public cloud environment. In the latter, seizing the data centres would unjustly impact on the other users, and may not lead to any result, as data may only

security practices would help to preserve the evidence…and/or avoiding further incidents deriving from negligence of data control (i.e. hacking into the police systems). In addition, "depending on the kind of investigation, it could be relevant to determine responsibility for (the lack of) security."[340]

"Likewise, cloud providers also have to establish procedures to respond to data access requests by LEAs in case of an investigation, or to DPAs' information requests on this point. As for users, cloud service providers do not often notify users of subpoenas when it is lawful to do so, even if they declare they will do so in their privacy policies."[341]

4.4.7 Exceptions to data protection rules: LEA purposes

This brings us to the final point: the access and use of data in the cloud for law enforcement purposes, which calls into question the adequacy of the existing framework, data transfers abroad and purpose creep.

When the EU accesses those data, it will be bound to respect the EU legislation. However, "the current general data protection legal framework in LEAs is not adequate. While Europol/Eurojust, as *leges speciales*, have a very comprehensive data protection system, questions of a legal nature arise when data are handled by MS, the 24/7 contact points activated by the G8 or the Cybercrime Convention."[342]

The cloud does not raise any additional problems relating to data processing in the former third pillar, besides the well-known ones. COM (2010) 609 acknowledged the limits of Council Framework Decision 2008/977/JHA for four reasons. Firstly, applying in practice the Decision to cross-border exchange of personal data within the EU, but not to domestic processing operations in the MS, is difficult in practice and challenges its implementation. Secondly, the exceptions to the purpose limitation principle are too wide. Thirdly, there is no provision whereby different categories of data should be distinguished in accordance with their degree of accuracy and reliability. Finally, the fact that it does not replace the various sector-specific legislative instruments may directly affect the possibilities for individuals to exercise their data protection rights in this area. Therefore, with a view to establishing a comprehensive and coherent system in the EU and vis-à-vis third countries, it called for an overhaul of the current rules in the AFSJ, which has been in fact proposed, in the form of a Directive.

The new Directive seems, *prima facie*, to offer many improvements. Firstly, the Directive applies to all processing made by any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, with the exception of EU institutions and processing falling outside the scope of EU law (article 3). Accordingly, the data protection rules pertaining to institutions such as Europol, Frontex and Eurojust are unaffected. Secondly, article 5 introduces a distinction between different categories of data subjects, which is novel in data protection law, and article 6 lays down rules on the different degrees of accuracy and reliability of personal data. It also lays down rules on profiling and the processing of sensitive data. An important innovation is the introduction of both the obligation to appoint a data protection offer (article 30) and, pursuant to article 39, a Supervisory Authority, which monitors the application of the provisions of the proposed Directive. However, given the high sensitivity of the matter, the final draft may change dramatically, and it is therefore too early to assess this proposal.

Beyond this discussion, there are two problems. Firstly, attributing jurisdiction when data are processed/providers are established in several locations. Secondly, the lack of mechanisms to prevent

(Contd.)

be available temporarily. Once they have been deleted, it will be difficult to prove their existence, as they are physically stored on the PC anymore.

[340] Porcedda, "Law Enforcement in the Clouds," p. 219.

[341] Ibid.; see also Bradshaw et al. "Contracts for Clouds."

[342] Porcedda, "Law Enforcement in the Clouds," p. 227.

third states breaching EU data protection standards when accessing data in the cloud relating to EU citizens, whether upon transfer of this data, or forced access.

As for data transfers abroad, when it comes to LEAs the general rule is to transfer data only to countries ensuring an adequate level of protection, subject to very restrictively interpreted exceptions. "However, while 'in principle' the Council Framework Decision 2008/977/JHA respects the idea (recital 23), in practice both article 13 on transfers to third states authorities/international bodies and article 26 (without prejudice to existing instruments) are very permissive."[343] Chapter V of the proposed Directive seems to follow the same philosophy. Then, access to the data may take place without an explicit data transfer following a declaration of adequacy. Disclosure may be ordered for law enforcement purposes. The provisions of the Patriot Act are a case in point. Electronic surveillance,[344] for instance for economic espionage, is another risk. This is of course a sensitive point for all public administrations considering to 'go cloud': the provider will have to be chosen carefully, as well as the modalities for the cloud. The ultimate owner of a cloud may be a government, which may therefore have access to all information stored therein.[345]

Finally, purpose creep – i.e. the practice of 'recycling' the data lawfully collected for a new purpose, without the free and informed consent of the data subject – is an unfortunate reality, which has spilled over the AFSJ. In fact, LEAs have started demanding permanent access to data, which have been collected by the private sector (for commercial purposes), whereas derogation of data protection rules should be limited in time and scope. Such practices, which raise serious concerns in terms of the principle of data quality criteria, have been growing in the past few years on the basis of the 'principle of cooperation'[346] between law enforcement agents and private companies for investigation purposes.[347]

One of the most well-known cases in the EU is the Data Retention Directive, which would not apply to most cloud computing services as they are ISS, as seen in 0. Purpose creep has also an international dimension, which sparked controversial cases such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT),[348] which is essentially a "private cloud for financial services."[349] The 'TFTP Agreement'[350] represents a substantial step in the direction of the creation of a domestic cloud, although it does not realise it completely. In fact, "from a privacy perspective in cloud computing, the location of the control (and effective processing) is more important than that of simple storage."[351]

The Communication recognises that the rights enshrined in article 8(2) of the EUCFR, i.e. data minimization and effective control of one's own data, are difficult to exercise online, and are enforced differently in different countries. In order to address this point, it proposed to clarify the "right to be forgotten" and to ensure data portability (the possibility to withdraw ones' data, such as photos or a list of friends, from an application or service so as to transfer them elsewhere, without the opposition of the data controllers). Indeed, the former is contained in article 17 of the proposed Regulation, whereas

---

[343] Porcedda, "Law Enforcement in the Clouds," p. 225.

[344] Clarke and Stavensson, *Privacy and Consumers Risks*; Gayrel et al. "Cloud Computing."

[345] Robert Gellman, "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing" (paper prepared for the World Privacy Forum, November 23, 2009).

[346] Ibid.; Dumortier et al., "La Protection des Données."

[347] For a detailed analysis of the public-private partnerships, see Porcedda, "Regulatory Challenges," Section 2.

[348] See at <https://www.privacyinternational.org/article/european-union-privacy-profile>.

[349] See: <http://www.swift.com/about_swift/press_room/swift_news_archive/2010/business_forum/Canadian_Business_Forum_2010.page>. Also, Sibos. "Sibos Issues Thursday. The official daily Newspaper of Sibos." Hong Kong, September 14-18, 2009.

[350] Agreement between the European Union and the United States of America, OJ L 195, 27.7.2010, p. 5–14.

[351] Porcedda, "Law Enforcement in the Clouds," p.228.

the latter is laid down by article 18. The principle of data minimisation has also been introduced by the proposed article 5(c).

4.4.8 Appraising the Communication and the proposed Regulation

On the basis of this brief analysis, the Communication, and the ensuing Regulation, seem to be moving overall in the right direction to meet the challenges of cloud computing. An exception is the definition of personal data, which I believe should be updated, in particular with a view to increasing the complementarity between privacy and data protection, and cyber-security. No matter how interlinked the two may be, if data protection laws were outdated, they would be of little help for cybercrime.

Certainly, it has to be seen how the proposed Regulation will survive the many reviews, and in particular the proposed Directive. Indeed, this is an area of convergence of policies produced by different Directorate Generals, which do not necessarily have the same policy orientations. Criticism has already been raised with regards to the proposed Directive.

This chapter has addressed the two caveats on privacy, namely adopting a core-periphery approach leading to better crafted data protection rules, and updating the data protection legislation in order to meet the challenges, especially the technological ones. I will now integrate the two and reach a conclusion.

5. Conclusions: A Dual Role for Cyber-Security Policy in the EU?

5.1 Introduction

The objective of this research was to contribute to the 'security vs. privacy' debate. In particular, it tried to theoretically demonstrate the existence of one instance where security and privacy can be complementary, namely the case of cybercrime and cyber-security. This is not to say that privacy and data protection are the key to solving the problems of cybercrime and cyber-security, but that they may be more a support than an obstacle, contrary to the zero sum game depicted by the classic dichotomy. I have tried to explain the links by using the EU legal framework as a practical example. I shall now try to address the question whether a 'human rights by design' security policy is feasible, and how, in a more direct manner. The burden of proof is on privacy, as in the 'security vs. privacy' debate, it is perceived as the obstacle to obtaining additional security.

5.2 Integrating Cyber-Security and Privacy

5.2.1 De facto

If one looks at the factual conditions of privacy and security in the cyber-realm, it is not difficult to show the integration of security and privacy.

"The canonical goals of information security[352] are confidentiality, integrity and availability…Integrity is a degree of confidence that the data (and system) is supposed to be there, and is protected against accidental or intentional alteration without authorization…(it) is supported by well audited code, well-designed distributed systems and robust access control mechanisms. Availability means being able to use the system as anticipated." Finally, "confidentiality refers to keeping data private. Privacy is of tantamount importance as data leaves the borders of the organization…(it) is supported by, among other things, technical tools such as encryption and access control, as well as legal protection."[353] The canonical goals apply both at the end point– the individual – and at the systemic level – the network. The latter is also the level of CII; therefore cyber-security, intended as the policy tackling CIIP, hinges on the application of the same goals. From here my first hypothesis, namely that narrow cybercrime and cyber-security pertain to the same phenomena, is descended.

Likewise, one of the FIPPs is 'security of the processing operations of the personal data'. If one can say that, by applying good confidentiality and integrity measures, privacy is defended, one could also say that, by applying good privacy measures, confidentiality and integrity are attained in part, as far as the personal data part is concerned. I have advanced the idea that, if the definition of data protection was extended, the complementarity of privacy and data protection rules would be increased accordingly, and in particular could apply to cyber-security at large. Therefore, a 'PbD' cyber-security policy is possible from a *de facto* perspective, provided that a technical view of security is adopted (first caveat). In this case, privacy would not only be a right, but a collective interest.[354]

If a national security view was endorsed instead, the pursuit of 'security' would entail surveillance, and privacy and data protection would be seen as the value opposed to security. Similarly, when one

---

[352] In practice, security is more nuanced than that, as "getting protection right…depends on several different types of processes. You have to figure out what needs protecting, and how to do it." Anderson, *Security Engineering*, p. 2.

[353] Allan F. Friedman and Darrell M. West, "Privacy and Security in Cloud Computing," *Issues in Technology Innovation*, n° 3 (2010).

[354] Bennett and Raab, *The Governance of Privacy*.

focuses on broad cybercrimes, privacy and data protection become a value to be balanced against prosecuting the crime. I have argued that this is because tackling broad cybercrime requires reactive measures, since the data are only an online 'projection' of a crime happening in the real world, and therefore constitute evidence, and not the object of the protection itself. As a consequence, broad and narrow cybercrimes are profoundly different in terms of underlying logics (first hypothesis).

5.2.2 De iure

The technical approach recognises the importance of regulation for the pursuit of confidentiality. Data protection and privacy laws, as they currently stand, can be divided into two groups: the rules which discipline cyber-crime and 'security' (as defined in the introduction) from the personal data perspective, which show 'complementarity', and the rules which impose obligations which 'contribute' to the prevention of cybercrimes and the pursuit of cyber-security.

Complementary rules to cybercrime and the pursuit of cyber-security

The first group includes the following:

- Article 16 of the Directive 95/46/EC and articles 5 of the e-Privacy Directive on confidentiality, and to a certain extent articles 6 on traffic data and 9 on location data other than traffic data, prohibit illegal interception of data, which is punished by article 6 of the proposed Directive on Attacks against Information Systems;
- The revised article 5.3 of the e-privacy Directive, which mandates to request the consent to install cookies, forbids illegal access to information systems, which is punished by article 3 of the proposed Directive;
- Article 13 of the e-privacy Directive proscribes spamming, which is an illegal system interference pursuant to article 4 of the proposed Directive;
- Article 17 of Directive 95/46 punishes illegal data interference (article 5 of the proposed Directive);
- Article 24 of Directive 95/46 on sanctions is in line with both articles 9 on penalties and 11 on liability of legal persons of the proposed Directive.

The same articles also proscribe computer fraud and forgery, i.e. articles 7 and 8 of the Cybercrime Convention, insofar as the data that is the object of the offence is considered personal within the meaning of article 2 of Directive 95/46/EC. The argument that the concept of personal data should be extended is also valid here.

Rules contributing to the prevention of crimes and cyber-security

There are two main categories of data, which can contribute to the prevention of cyber-crime and the pursuit of cyber-security.

- Article 17 of the Directive 95/46/EC creates preventive measures for all offences which involve a breach of security, as addressed by articles 3 to 6 of the proposed Directive on Attacks against Information Systems, thanks to the obligation to adopt the necessary organizational and technical measures, which must be appropriate to the risks posed by the processing activity, provided these are technically and economically feasible for the controller or the processor (which must in turn be chosen in an accurate manner).
- Examples of appropriate technical security measures are: an adequate information management system to control access to data; this includes the use of audit trails, which allow logs to be kept; the use of PETs and protection against breaches, for example through the use of patches,

encryption etc.; the obligation to segregate the data stored; and maintaining a person responsible for security.[355]

- Proposed procedural measures include: obligations to audit the system (and keep audit-trails); cooperation between service providers and DPAs (allowing audit of security measures/issuance of recommendations); and a security policy expressed in clear language.[356]

Measures adopted in accordance with this article, and in particular the creation of logs and audit trails, have an additional, important effect: they are particularly valuable in case of an investigation, as they allow to limit the volatility of the data. This brings evidence to the claim that data protection rules are not necessarily at odds with an investigation concerning cybercrime.

- Article 4 of the e-privacy Directive on ensuring the security of the networks (now applicable also to public communications networks, following the innovation of the Telecom Package), in addition to what was stated above for article 16/ 13 of the e-privacy Directive, creates a preventive measure for system interference, including non-commercial spamming and DDoS attacks (a common example of cyber-attack);
- The new article 4.3 of the e-Privacy Directive on mandatory notification of data breaches is particularly important to fill the gap between misaligned incentives, i.e. the fact that those who should provide security – i.e. the producers – are not those needing it (the users); the latter are often unaware of such a need or assume protection *de facto*.[357] The measure introduces legal and social incentives, i.e. the obligation to report, the fear of customers' loss of confidence, as well as encourages the use of preventive techniques: if encryption is in place, the service is not obliged to report.
- The new article 5.3 has sparked a rush to compliance for a transparent use of cookies. This is helpful in preventing illegal interception.

Provided that the rules governing data protection are aligned with the technological reality (as it seems form the first version of the Regulation), that is, provided that caveat 3 is respected, privacy and security can be integrated. Privacy and data protection, actually, fill in the gap of preventive measures in cybercrime legislation, which is crucial due to the problem of attribution.

Further integration may come from a revision of the concept of personal data, which included legal persons. Another relevant aspect for those laws which discipline the same offences envisaged by the Directive repealing the Council Framework Decision on Attacks against Information Systems is that the coherency and certainty of law should be ensured.

In addition to the benefits created by log and audit trails, real complementarity with the rules can be ensured, then, provided that a core-periphery approach to privacy and data protection is adopted (which translates into the adoption of meaningful data protection rules in the area of police and judicial cooperation). Therefore, further research is needed to assess to what extent the safeguarding of personal data and privacy may be at odds with the objectives of an investigation, and therefore require 'balanced maximisation.' This is especially the case for what concerns broad cybercrime(s).

Finally, all measures pertaining to privacy and data protection hinge on the idea that data subjects are clearly and comprehensively informed, i.e. they are conscious of the purposes and objectives of the data collection and processing activities, and can then choose freely what level of protection they want to enjoy (so-called fully informed and freely given consent). Raising awareness for privacy and security are, in the end, two sides of the same coin. This link is missing in the Commission's proposal; with the increasing attention to broad cybercrime and CIIP as a national security issue, measures in the

[355] Gayrel et al. "Cloud Computing."

[356] Porcedda, "Law Enforcement in the Clouds."

[357] EDPS, *Opinion on Privacy by Design*.

opposite direction may be pursued. Therefore, to address 'how a EU cyber-security policy may integrate privacy and data protection', the accent should be put on preventive measures, raising awareness, and distributing responsibility at all levels, i.e. imposing the markets obligations to a minimum level of quality of the services offered, while reducing the impact of blanket surveillance measures, and the use of informal practices (i.e. PPPs) without strict guidelines, which threaten transparency. In the next paragraph, I will try to evaluate the likelihood of such an approach, given current trends in the EU.

5.3 Modalities of Integration: Mixed Evidence from Policy

On the one hand, the EU is taking the right approach towards cyber-security and cybercrime. The intention to mandate the creation of statistics, an appropriate reporting system, and information on the types of offences, all lead to the creation of evidence and, therefore, a clearer vision of the complex phenomenon of cybercrime. In particular, this should hopefully lead to a better understanding of the relative incidence of the different cybercrimes, and therefore to the adoption of more adequate and weighted policy choices over the measures to take (cryptography, the degree of secrecy or disclosure, anonymity, deep packet inspection, freedom of speech and so on). Additional consciousness on cyber-attacks and cyber-security is welcome as, indeed, our society relies on information and networks security for various critical services.

However, the decision to refer to the Cybercrime Convention despite its limits, combined with the spirit of latest policy documents, which tend to securitise the problem and put forward a classical security vision, and an opposition of rights and security, are worrying, especially if combined with the international trends on the matter.

For instance, the EU-US Working Group on Cybersecurity and Cybercrime (hereafter the WGCC) following the acknowledgement of the 'growing challenge of cyber-security and cyber-crime,'[358] should be scrutinized.[359] The WGCC has crucial objectives, among them 'consider(ing) options for outreach to other regions or countries addressing similar issues to share approaches and related activities and avoid duplication of effort.'[360] In other words, it aims to shape the global debate on the matter of cyber-security and cybercrime. If one looks at the recent history of EU-US relations in the area of home affairs, one probably does not hazard much in saying that the US approach may prevail, especially considering that the US has a more developed policy in cyber-security, which is bound to progress due to the considerable prospective investment on cyber security: $10.5 billion/year by 2015.[361]

This is certainly welcome as far as best practices are concerned, such as its crime reporting system, and the steps taken towards mandatory reporting of data breaches (which in the EU is a privacy issue). Yet, other trends are less encouraging. The military is gaining more power in cyber-security, with the contribution of the threat inflation produced by the media, sometimes silently supported by vested interests:[362] maintaining high levels of alert is convenient, since increased cyber security spending

---

[358] Council. EU-US Summit Joint Statement. 16726/10 Presse 315, Lisbon, 20 November 2010. p. 3.

[359] Commissioner Malmström, *Answer on behalf of the Commission to question by Marietje Schaake* (ALDE) of 17 May 2011, available at <http://www.statewatch.org/whatsnew.htm> (last accessed on 21 July 2001).

[360] Commissioner of, *Answer on behalf of the Commission to question by Ernst Strasser* (PPE) of 20 December 2010, 15 February 2011.

[361] Jerry Brito and Tate Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy." Mercatus Center, George Mason University, 26 April 2011.

[362] For different positions on the likelihood of cyber-wars, see: Giampiero Giacomello, "Minacce Digitali, Rischio Reale: Semplice Mito o Scenario Prossimo Venturo?" in *Introduzione al Mondo Nuovo*, ed. Fabio Armao (Milano: Guerini, 2006); Sommer and Brown, *Reducing Systemic Cybersecurity Risks*; Jerry Brito and Tate Watkins, Loving the Cyber Bomb?".

could compensate for budget cuts in other areas of defence, as well as to other governmental agencies, to gain more power. Representatives seem to be backing such approach as cyber-security represents a pork-barrel spending opportunity to create jobs and funds in their constituency.[363] Programmes like Einstein 2.0 and 3.0 recall too closely Total Information Awareness, which led to the disaster of the PNR Agreements.[364]

Moreover, despite its more stringent rules on privacy and data protection, the EU may not be more protective vis-à-vis the US.[365] The 2011 G8 forum can be considered a good barometer as regards the orientation of some of the most influential MS; several parties lamented the freedom restrictive approach adopted, either for economic or political concerns.[366] For instance, there seems to have been a recent cooperation with China on approximating practices on censoring illegal material on the Internet.[367] China's approach to the Internet is hardly known as being amongst the most liberal. These may be in line with the idea of creating a 'virtual Schengen border' and 'virtual access points', which entail the compilation of "black lists" by the Internet Service Providers, in order to block illicit content.[368] In other instances, the Commission's 'wait and see' approach, adopted in the case of net neutrality and filtering, may be equally damaging, as it allows dubiously lawful practices to take root and multiply, to the detriment of a culture of privacy and data protection, which would be beneficial to cyber-security. The evidence is mixed. The point is, privacy has a window of opportunity to be made not just relevant, but indispensable, and it would be a pity to miss such a chance.

5.4 Future Research

This research investigated the theoretical feasibility of integrating privacy and data protection with cyber-crime prevention and the pursuit of cyber-crime. In order to prove this in reality, practical research is needed, based on concrete evidence. In particular, it should be necessary to trace a map of all possible offences encompassed by the term cyber-crime, confirming whether the forensic practices are the same, and in particular seeing how the prevention and prosecution of each of them would interact with the others.

One way may be trying to map the attitudes of a number of representative governmental agencies and businesses towards privacy and security, by means of a sample interview to be conducted off-the-record. The data thus collected should be coded and then statistically processed through simple linear regression, to find the correlation between the two independent variables (privacy and security measures), to see if they are coordinated. In order to observe what made the difference in ICT based crimes prevention (dependent variable), the most relevant cases could be selected and process-traced. Other ways may be found to build the data-set and analyse it; what matters is to attempt to carry out the research in practice.

---

[363] Ibid.

[364] Porcedda, *Transatlantic Approaches to Cybersecurity*.

[365] On the topic, see Patryk Pawlak, "The Unintentional Development of the EU's Security Governance and Beyond Borders." *European Foreign Affairs Review* 17, Special Issue 2/1 (2012): 87–107.

[366] European Digital Rights (EDRi). G8 And E-G8 Summit On Internet Freedom. *Edri-gram* 9.11 (2011); G8 Declaration. *Renewed Commitment for Freedom and Democracy*. G8 Summit of Deauville, 26-27 May 2011.

[367] EDRi. "EU And China Adopt Harmonised Approach To Censorship." *Edri-gram*, 9.10 (2011).

[368] Council. *Outcome of Proceedings of the Joint meeting of the Law Enforcement Working Party and the Customs Cooperation Working Party (Virtual Schengen)*. 7181/11, 3 March 2011.

6. Bibliography

6.1 Literature

Ackerman, Bruce. *Before the Next Attack. Preserving civil liberties in an age of terrorism*. New Haven: Yale University Press, 2006.

Armbrust, Michael, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Konwinski Andrew, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica and Matei Zaharia. "Above the Clouds: A Berkeley View of Cloud Computing." Technical Report No. UCB/EECS-2009-28, University of California, Berkeley, 2009.

Anderson, Ross. *Security Engineering. A Guide to Building Dependable Distributed Systems*. Indianapolis: Wiley, 2008.

Anderson, Ross and Steven J. Murdoch. "Tools and Technology of Internet Filtering." in *Access Denied: The Practice and Policy of Global Internet Filtering*, edited by Ron Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain. Cambridge: The MIT Press, 2008.

Anderson, Ross and Moore, Tyler. "The Economics of Information Security," *Science*, 314 (2006): 610-613.

Arthur, Charles. "Google's problem is that it now believes itself above others – even governments." *Guardian.co.uk*, 1 May 2012, available at: http://www.guardian.co.uk/technology/2012/may/01/google-street-view-data-fcc?INTCMP=ILCNETTXT3487.

Balkin, Jack M., James Grimmelmann, Eddan Katz, Nimrod Kozlovski, Shlomit Wagman, and Tal Zarsky, editors. *Cybercrime. Digital Cops in a Networked Environment*. New York University Press, 2007.

Barcelo, Rosa. "EU: Revision of the ePrivacy Directive." *Computer Law Review International* 5, (2009): 129 – 160.

Bennet, Colin, and Charles Raab. *The Governance of Privacy. Policy Instruments in a Global Perspective*. Cambridge: The MIT Press, 2006.

Bradshaw, Simon. "Cloud Computing: Security and Privacy Aspects and Cloud Contracts." Conference presentation. Ankara, May 2010.

Bradshaw, Simon, Christopher Millard and Ian Walden. "Contracts for Clouds: A Comparative Analysis of Terms and Conditions for Cloud Computing Services." Queen Mary School of Law Legal Studies Research Paper No. 63/201, London, 2010.

Brito, Jerry and Tate Watkins. "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy." Mercatus Center, George Mason University, April 2011, available at: http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy.

Brenner, Susan and Bert-Jaap Koops, editors. *Cybercrime and Jurisdiction. A Global Survey*. The Hague: TMC Asser Press, 2006.

Buzan, Barry, Ole Weaver and Jaap De Wilde. *Security: a New Framework for Analysis*. Boulder: Lynne Rienner, 1998.

Cavoukian, Ann. *Privacy by Design…Take the Challenge*. Information and Privacy Commissioner of Ontario, Canada, available at: http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf.

Cassim, Fawzia. "Formulating Specialised Legislation to Address the Growing Specter of Cybercrime: a Comparative Study." *Potchefstroom Electronic Law Journal* 12, n° 4 (2009).

Clarke, Roger, and Dan Stavensson. "Privacy and Consumers Risks in Cloud Computing." *Computer Law and Security Review* 26, n°4 (2010): 391-397.

Clough, Jonathan. *Principles of Cybercrime*. Cambridge: Cambridge University Press, 2010.

Commission Nationale de l'Informatique et des Libertés (CNIL). "Google Street View : CNIL pronounces a fine of 100,000 Euros." March 2011, available at: <http://www.cnil.fr/english/news-and-events/news/article/google-street-view-cnil-pronounces-a-fine-of-100000-euros/>.

Cremona, Marise. "The Two (or Three) Treaty Solution: The New Treaty Structure of the EU" in *European Union Law After the Treaty of Lisbon*, ed. By Andrea Biondi. Piet Eeckhout and Stephanie Ripley (Oxford: Oxford University Press 2012).

De Busser, Els. *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities*. Maklu Uitgevers N.V., 2009.

De Hert, Paul and Serge Gutwirth. "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action." In *Reinventing Data Protection?* Edited by Serge Gutwirth, Yves Poullet, Paul De Hert, Sjaak Nouwt and Cécile de Terwangne, 3-44. Springer, 2009.

De Hert, Paul, Vagelis Papakonstantinou and Cornelia Riehle. "Data Protection in the Third Pillar: Cautious Pessimism." In *Crime, Rights and the EU, the Future of Police and Judicial Cooperation*, edited by Martin Maik. London: Justice, 2008.

De Rosa, Mary. "Data Mining and Data Analysis for Counterterrorism." Center for Strategic and International Studies, March 2004, available at: http://csis.org/files/media/csis/pubs/040301_data_mining_report.pdf.

Diffie, Withfield, and Susan Landau. "Internet Eavesdropping: A Brave New World of Wiretapping." *Scientific American Magazine*, September 2008.

Donhoue, Laura K. *The Cost of Counterterrorism, Power, Politics, and Liberty*. New York: Cambridge University Press, 2008.

Dumortier, Frank, Claire Gayrel, Yves Poullet, Joëlle Jouret, Damien Moreau. "La Protection des Données dans l'Espace Européen de Liberté, de Sécurité et de Justice." *Journal de Droit Européen* 166 (2010): 33- 46.

Eckstein, Harry. "Case Study and Theory in Political Science." in *Handbook of Political Science*, edited by Fred I. Greenstein and Nelson W. Polsby, Vol. 3. Reading: Addison-Wesley, 1975.

Essers, L. "Dutch Court Rules WiFi Hacking is Now Legal", *Pcworld.com*, 18 March 2011, available at: <http://www.pcworld.com/article/222589/dutch_court_rules_wifi_hacking_is_now_legal.html> and at: *EDRi-gram* 9.6 (2011): <http://www.edri.org/edrigram/number9.6/court-Wifi-hacking-legal-netherlands>.

European Digital Rights (EDRi). G8 And E-G8 Summit On Internet Freedom. *Edri-gram* 9.11 (2011), available at: <http://www.edri.org/edrigram/number9.11/g8-internet-freedom>;

EDRi. "EU And China Adopt Harmonised Approach To Censorship." *Edri-gram*, 9.10 (2011), available at: <http://www.edri.org/edrigram/number9.10/eu-china-censorship-internet>.

EDRi, "German Supreme Court Fines Owner of Open WiFi Network", *Edri-gram*, 8.10 (2010), available at: <http://www.edri.org/edrigram/number8.10/wifi-case-germany-copyright-infringement>.

Edwards, Lilian and Charlotte Waelde, editors. *Law and the Internet*. Portland: Hart Publishing, 2009.

Etzioni, Amitai. *How patriotic is the Patriot Act*. New York and London: Routledge, 2004.

Friedrichs, Jörg and Friedrich Kratochwil. "On Acting and Knowing: How Pragmatism Can Advance International Relations Research and Methodology." *International Organization* 63 (2009): 701–31.

Friedman, Allan F. and Darrell M. West. "Privacy and Security in Cloud Computing." *Issues in Technology Innovation*, 3 (2010).

Gayrel, Claire, Jacques Gérard, Jean-Philippe Moniy, Yves Poullet, Jean-Marc Van Gyseghem. "Cloud Computing and its Implications on Data Protection." Paper for the Council of Europe's project on Cloud Computing, Centre de Recherche Informatique et Droit, Namur, March 2010, available at: <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1b.pdf>.

Gellman, Robert. "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing." Paper prepared for the World Privacy Forum, November 2009.

Giacomello, Giampiero. "Minacce Digitali, Rischio Reale: Semplice Mito o Scenario Prossimo Venturo?" in *Introduzione al Mondo Nuovo*. Edited by Fabio Armao and Anna Caffarena. Milano: Guerini, 2006.

Grance, Tim and Peter Mell. "The NIST Definition of Cloud Computing." Version 15, July 2009, available at:<http://csrc.nist.gov/groups/SNS/cloud-computing/>.

Hijmans, Hielke and Alfonso Scirocco. "Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to Help?" *Common Market Law Review* 46 (2009): 1485-1525.

Hustinx, Peter. "Data Protection and Cloud Computing under EU Law." Speech delivered at the Third European Cyber Security Awareness Day, Brussels, April 2010.

___. "Data protection in the light of the Lisbon Treaty and the Consequences for Present Regulations." Speech delivered at the 11th Conference on Data Protection and Data Security, Berlin, 8 June 2009.

Krause, Catarina and Martin Scheinin. editors. *International Protection of Human Rights: a Textbook*. Turku: Abo Akademi Institute for Human Rights, 2009.

Kshetri, Nir. *The global Cybercrime Industry. Economic, Institutional and Strategic Perspectives*. Springer, 2010.

___. "Information and Communication Technologies, Strategic Asymmetry and National Security." *Journal of International Management*, 11, n° 4 (2005).

Kushida, Kenji, Jonathan Murray and John Zysman. "Diffusing the Fog: Cloud Computing and Implications for Public Policy." BRIE Working Paper 197, March 2011.

Landau, Susan. Surveillance or Security? *The risk Posed by New Wiretapping Technologies*. Cambridge: the MIT Press, 2010.

Lawless, Robert M. et al. *Empirical Methods in Law*. Aspen Publishers, 2010.

Leenes, Ronald. "Who Controls the Cloud?" *Revista de Interent, Derecho y Politica* 11 (2010).

Lijphart, Arend. "Comparative Politics and the Comparative Method." *American Political Science Review* 65, n° 3 (1971): 682-693.

Lixinski, Lucas. "Legal Implications of the Privatization of Cyber warfare." Academy of European Law, EUI Working Paper, Priv-war Project, AEL 2010/02, 2010.

Lohr, Steve. "The Age of Big Data." *Nytimes.com*, 18 February 2012, available at https://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?_r=1&ref=technology.

Moses, Asher. "'Petulant' Conroy accuses Google of 'single greatest privacy breach'." *Smh.com.au*, 25 May 2010, available at: <http://www.smh.com.au/technology/technology-news/petulant-conroy-accuses-google-of-single-greatest-privacy-breach-20100525-w937.html>.

Nash, Victoria and Malcolm Peltu. "Rethinking Safety and Security in a Networked World: Reducing harm by Increasing Cooperation." Forum Discussion Paper N° 6, Oxford Internet Institute, November 2005.

Newman, Abraham L. *Protectors of Privacy. Regulating Personal Data in the Global Economy*. Ithaca: Cornell University Press, 2008.

Nielsen, Nikolaj. "EU cyber-security legislation on the horizon." *Euobserver.com*, 11 May 2012, available at: < http://euobserver.com/22/116239>.

O'Brien, Kevin J. "European Regulators May Reopen Street View Inquiries." *Nytimes.com*, 2 May 2012, available at: <https://www.nytimes.com/2012/05/03/technology/european-regulators-to-reopen-google-street-view-inquiries.html?_r=1&pagewanted=2&src=un&feedurl=http://json8.nytimes.com/pages/technology/index.jsonp>.

Pawlak, Patryk. "The Unintentional Development of the EU's Security Governance and Beyond Borders." *European Foreign Affairs Review* 17, Special Issue 2/1 (2012): 87–107.

Porcedda, Maria Grazia. "Law enforcement in the clouds: is the EU data protection legal framework up to the task?" in *Data Protection in Good Health*, edited by Serge Gutwirth, Paul de Hert, Ronald Leenes and Serge Gutwirth. Springer, 2012.

___. "Transatlantic approaches to cyber-security: the EU-US Working Group on Cyber-security and Cybercrime." In *The EU-US security and justice agenda in action*, edited by Patryk Pawlak, Chaillot Paper. Paris: EUISS, December 2011.

Porcedda, Maria Grazia and Ian Walden. "Regulatory Challenges in a Changing Computing Environment." Working paper for the Conference "Law Enforcement in the Clouds: Regulatory Challenges" Brussels, Belgium, 24 February 2011, available at: <http://www.crid.be/cloudcomputing/default.htm>.

Posner, Richard A. "Legal Scholarship Today." *Harvard Law Review* 115 (2002): 1314–26;

Leonardo Rapone. *Storia dell'Integrazione Europea*. Roma: Carocci, 2004.

Rodotà, Stefano. *Intervista su Privacy e Libertà*. A cura di Paolo Conti, Laterza, 2005.

___. "Data Protection as a Fundamental Right." In *Reinventing Data Protection?* edited by Serge Gutwirth, Yves Poullet, Paul De Hert, Sjaak Nouwt and Cécile de Terwangne. Springer, 2009.

___.*Elaboratori Elettronici e Controllo Sociale*. Mulino: Bologna, 1973.

Rosenzweig, Paul. "Privacy and counter-terrorism: the pervasiveness of data." *Case Western Reserve Journal of International Law* 42 (2010): 625-646.

Sartor, Giovanni. "Doing Justice to rights and values: teleological reasoning and proportionality." *Artificial Intelligence and Law* 18, n°2 (2010) :175-215.

___. *L'informatica Giuridica e le tecnologie dell'informazione*. *Corso di Informatica giuridica*. Torino: Giappichelli Editore, 2010.

Scheinin, Martin. "Terrorism and the Pull of 'Balancing' in the Name of Security." In *Law and Security - Facing the Dilemmas*, edited by Martin Scheinin, European University Institute Working Paper No.11. Florence: European University Institute, 2009.

Schneier, Bruce. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. Springer, 2003.

Sibos. "Sibos Issues Thursday. The official daily Newspaper of Sibos." Hong Kong, September 14-18, 2009.

Smits, Jan M. "Redefining Normative Legal Science." in *Methods of Human Rights Research*, edited by Fons Coomans, Fred Grunfeld and Menno Kamminga, 45-58. Antwerp: Oxford, 2009.

Solove, Daniel J. " 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy." GWU Law School Public Law Research Paper No. 289 and *San Diego Law Review* 44 (2007): 745.

Sommer, Peter and Ian Brown. "Reducing Systemic Cybersecurity Risks." OECD/IFP Project on 'Future Global Shocks'. Paris: OECD, 2011.

Streitfeld, David and Kevin J. O'Brien. "Google Privacy Inquiries get little cooperation." *Nytimes.com*, 22 May 2012, available at: <http://www.nytimes.com/2012/05/23/technology/google-privacy-inquiries-get-little-cooperation.html?_r=1&hp&pagewanted=all>.

Swire, Peter and Lauren Steinfeld. "Security and Privacy After September 11: The Health Care Example." *Minnesota Law Review* 86 n° 6 (2002): 1515-40.

Van Evera, Stephen. *Guide to Methods for Students of Political Science*. Cornell University Press, 1997.

Vick, Douglas W. "Interdisciplinarity and the Discipline of Law." *Journal of Law and Society*, 31 (2004): 163–93.

Viola de Azevedo Cunha, Mario. "The Concept of Personal Data in the Post Lisbon era: is there need (and room) for change?" in *Data Protection in Good Health?* Edited by Serge Gutwirth Paul de Hert, Ronald Leenes and Serge Gutwirth. Springer, 2012.

Waxman, Matthew C. "Cyber-attacks and the Use of Force - Back to the Future of Article 2(4)." Columbia Law School Working Paper, September 2010.

6.2 Legal Instruments and Policy Documents

Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program. OJ L 195, 27.7.2010, p. 5–14.

Article 29 Data Protection Working Party. "Opinion 15/2011 on the Definition of Consent." (WP 187), Brussels, 13 July 2011.

___. "Working Document 01/2011 on the Current EU Personal Data Breach Framework and Recommendations for Future Policy Developments." (WP 184), Brussels, 5 April 2011.

___. "Opinion 3/2010 on the Principle of Accountability." (WP 173), Brussels, July 2010.

___. "Report 01/2010 on the Second Joint Enforcement Action: Compliance at National Level of Telecom Providers and ISPs with the Obligations Required from National Traffic Data Retention Legislation on the Legal Basis of Articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC Amending the e-Privacy Directive." (WP 172), Brussels, July 2010.

___. and The Working Party on Police and Justice, "'The Future of Privacy': Joint contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data." (WP 168), Brussels, December 2009.

___."Opinion 1/2010 on the Concepts of 'Controller' and 'Processor.'" (WP 169), Brussels, February 2010.

___. "Opinion N. 4/2007 on the Concept of Personal Data." (WP 136), Brussels, June 2007.

___. "Opinion 9/2001 on the Commission Communication on 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime'." (WP 51), Brussels, 5 November 2011.

___. "Opinion 4/2001 On the Council of Europe's Draft Convention on Cybercrime." (WP 41), Brussels, March 2001.

___. "Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU data protection directive." (WP 12), July 1998.

Charter of Fundamental Rights of the European Union. OJ C 364, 18.12.2000, p. 1–22.

Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU). OJ C 83, 30.3.2010.

Commissioner Malmström. *Answer on behalf of the Commission to Question by Marietje Schaake (ALDE) of 17 May 2011*. available at: <http://www.statewatch.org/whatsnew.htm>.

Commissioner Reading. *The Review of the EU Data Protection Framework*. SPEECH/11/183, Brussels, 16 March 2011.

Commissioner Kroes, *Answer on behalf of the Commission to question by Ernst Strasser* (PPE) *of 20 December 2010*, 15 February 2011.

Council of Europe. *Additional Protocol Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems*. ETS n°189, Strasbourg, 28 January 2003.

___. Convention on Cybercrime. CETS n° 105, Budapest, 23 November 2001.

___. *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows*. CETS No. 181, Strasbourg, 8 November 2001.

___. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. CETS No. 108, Strasbourg, 28 January 1981.

___. *Recommendation of the Committee of Ministers regulating the use of Personal data in the Police Sector (Police Recommendation). R (87) 15*, Strasbourg, 17 September 1987.

___. *Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No 11 and 14*. CETS n° 005, Rome, 4 November 1950.

Council of the European Union and European Commission. *Council and Commission Action Plan implementing the Hague Programme on strengthening Freedom, Security and Justice in the European Union*. OJ C 198, 12.8.2005, p. 1-22.

Council Conclusions of 27 November 2008 on a concerted strategy and practical measures against cybercrime. OJ C 62, 17.3.2009, p. 16-18.

Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and Amending Decision 2002/187/JHA Setting up Eurojust with a View to Reinforcing the Fight against Serious Crime. OJ L 138, 4.6.2009, p. 14–32.

Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol). OJ L 121, 15.5.2009, p. 37–66.

Council Decision No 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 Establishing a Multiannual Community Programme on Protecting Children Using the Internet and other Communication Technologies. OJ L 348, 24.12.2008, p. 118-127.

Council Decision of 29 May 2000 to combat child pornography on the Internet. OJ L 138, 9.6.2000, p. 1-4.

Council. *Draft Council conclusions on an Action Plan to implement the concerted strategy to combat cybercrime*. 5957/2/2010, Brussels, 25 March 2010.

Council. *Draft Internal Security Strategy for the European Union: Towards a European Security Model*. 5842/2/10, Brussels, 23 February 2010.

Council. *Draft Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime*. 15569/08, Brussels, 11 November 2008.

Council. *EU Action Plan on Combating Terrorism*. 15893/10, Brussels, 15 November 2010.

Council. *EU-US Summit Joint Statement*. 16726/10 Presse 315, Lisbon, 20 November 2010.

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.

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. OJ L 69, 16.03.2005, p. 67-71.

Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography. OJ L 13, 20.01.2004, p. 44-48.

Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment. OJ L 149, 2.6.2001, p. 1–4.

Council. *Outcome of Proceedings of the Joint meeting of the Law Enforcement Working Party and the Customs Cooperation Working Party (Virtual Schengen)*. 7181/11, 3 March 2011.

Council. *Presidency Conclusions of the Cybercrime Conference (Budapest Conclusions)*. Budapest, April 12-13 2011, available at: http://www.statewatch.org/news/2011/may/eu-council-budapest-conclusions-cyber-wall.pdf.

Council. *Presidency Conclusions, Brussels European Council 21/22 June 2007*. 11177/1/07, 20 July 2007.

Council. *Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, replacing Council Framework Decision 2005/222/JHA.* 11566/11, Brussels, 15 June 2011.

Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security. OJ C 321, 29.12.2009, p. 1-4.

Council Resolution of 22 March 2007 on a Strategy for a Secure Information Society in Europe. OJ C 068, 23.3.2007, p. 1-4.

Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security. O JC 48, 28.02.2003, p. 1-2.

Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security. OJ C 43, 16.2.2002, p. 2-4.

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. OJ L 337, 18.12.2009, p. 11–36.

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

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, 31.07.2002, p. 37-47.

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.

European Commission. *Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*. COM (2012) 10 final, 25 January 2012.

___. *Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. COM (2012) 11 final, 25 January 2012.

Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions (Communication from the Commission). *The open internet and net neutrality in Europe*. COM(2011) 222 final, 19 April 2011.

Communication from the Commission. *Achievements and next steps: towards global cyber-security*. COM (2011) 163 final, 31 March 2011.

Communication from the Commission. *The EU Internal Security Strategy in Action; Five steps towards a more secure Europe*. COM (2010) 673 final, 22 November 2010.

Communication from the Commission. *A Comprehensive Approach on Personal Data Protection in the European Union*. COM (2010) 609 final, 4 November 2010.

Communication from the Commission. *Proposal for a Directive on Attacks against Information Systems and repealing Council Framework Decision 2005/222/JHA*. COM (2010) 517 final, 30 September 2010.

Communication from the Commission. *The EU Counter-Terrorism Policy: main achievements and future challenges*. COM (2010) 386 final, 20 July 2010.

Communication from the Commission. *Overview of information management in the area of freedom, security and justice*. COM (2010) 385 final, 20 July 2010.

Communication from the Commission. *A Digital Agenda for Europe*. COM (2010) 245 final, 19 May 2010.

Communication from the Commission. *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*. COM (2009) 149 final, 30 March 2009.

Communication from the Commission. *Towards a general policy on the fight against cyber crime*. COM (2007) 267 final, 22 May 2007.

Communication from the Commission. *Promoting Data Protection by Privacy Enhancing Technology (PETs)*. COM (2007) 228 final, 2 May 2007.

Communication from the Commission. *A strategy for secure information Society- dialogue, partnership an empowerment*. COM (2006) 251 final, 31 May 2006.

Communication from the Commission. *Green Paper on a European Program for Critical Infrastructure Protection*. COM (2005) 576 final, 17 November 2005.

Communication from the Commission. *Network and Information Security: Proposal for A European Policy Approach*. COM (2001) 298 final, 6 June 2001.

Communication from the Commission. *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating - Computer-related Crime*. COM(2000) 890 final, 26 January 2001.

Communication from the Commission. *Growth, Competitiveness, Employment. The Challenges and Ways forward into the 21st Century. White Paper*. COM (93) 700, 5 December 1993.

European Council. *Report on the Implementation of the European Security Strategy– Providing Security in a Changing World (European Security Strategy)*. Brussels, S407/08, 10 December 2008.

___. *A secure Europe in a better world (European Security Strategy)*. Brussels, 12 December 2003.

Regulation 542/2010 of 3 June 2010 amending Decision 2008/839/JHA on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II). OJ L 155, 22.6.2010, p. 23–26.

Regulation 460/2004/EC of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. OJ L 077, 13.3.2004. p. 1-11.

Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. OJ L8, 12.1.2001, p. 1-21.

European Court of Human Rights. *Case* 28957/95: *Christine Goodwin v. UK. Judgement*, 11.7.2002.

___. Case 20605/92: *Halford v. UK. Judgement*, 25.6.1997.

European Court of Justice. *Case C-301/06: Judgment of the Court (Grand Chamber) of 10 February 2009 — Ireland v. European Parliament, Council of the European Union*. OJ C 82, 4.4.2009, p. 2–3.

European Data Protection Supervisor (EDPS). *Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy (Opinion on Privacy By Design)*. OJ C 280, 16.10.2010, p. 1–15.

___. *Opinion on Net Neutrality, Traffic Management and the Protection of Privacy and Personal Data*. OJ C 34, 8.2.2012, p. 1–17.

European Defence Agency. *Bridging Efforts (Conference). Connecting Civilian Security and Military Capability Development*. Bulletin 14, May 2010.

European Network and Information Security Agency (ENISA). *Cloud Computing, Benefits, Risks and Recommendations for Information Security*. Crete, November 2009.

___. *National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace*. Crete, May 2012.

___. *Recommendations on Technical Implementation Guidelines of Article 4*. Crete, April 2012.

G8 Declaration. *Renewed Commitment for Freedom and Democracy*. G8 Summit of Deauville, 26-27 May 2011, available at: <http://www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html>

G8 Government and Industry Conference on High-Tech Crime. *Report of Workshop 3: Threat Assessment and Prevention*. Tokyo, 22-24 May 2001, available at <http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-6.html>.

High-Level Group on the Information Society. *Recommendations to the European Council. Europe and the global information society (The Bangemann Report)*. 26 May 1994.

House of Lords. *Protecting Europe against large-scale cyber-attacks*. European Union Committee, 5th Report of Session 2009-10, 18 March 2010.

___. *Follow up to the Personal Internet Security Report*. Science and Technology Committee, 4th Report of Session 2007-08, 8 July 2008.

___. *The Treaty of Lisbon: An Impact Assessment*. European Union Committee, 10th Report of Session 2007-2008, 13 March 2008.

___. *Personal Internet Security*. Science and Technology Committee, 5th Report of Session 2006-07, 10 August 2007.

The EU Security Roundtable. *European Cyber Security Conference Shared Threats – Shared Solutions: Towards a European Cyber Security Policy*. Conference Report, 14 June 2011, available at: http://www.security-round-table.eu/conf_conference_cyber11.php.

The Stockholm Programme. An open and secure Europe serving and protecting citizens. OJ C 115, 4.5.2010, p. 1-38.

United Nations. *Letter to the United Nations addressed to the Secretary General*, General Assembly. A/66/359, 14 September 2011.

___. *Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes*. New York: Counter-Terrorism Implementation Task Force (CTITF), 2009.

White House. *President's Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. 2009.

This working paper is based on research conducted within the Framework 7 projects SurPRISE and SURVEILLE, funded by the European Commission.