Cybersecurity and Privacy Rights in EU Law.

Moving beyond the trade-off model to appraise the role of technology

Maria Grazia Porcedda

Thesis submitted for assessment with a view to obtaining
the degree of Doctor of Laws of the European University Institute

Florence, 30 March 2017.

European University Institute
Department of Law

Cybersecurity and Privacy Rights in EU Law.

Moving beyond the trade-off model to appraise the role of technology

Maria Grazia Porcedda

Thesis submitted for assessment with a view to obtaining
the degree of Doctor of Laws of the European University Institute

Examining Board

Professor Marise Cremona, (EUI Supervisor)
Professor Deirdre Curtin, EUI
Professor Anne Flanagan, Queen Mary University of London
Professor Ronald Leenes, Tilburg University

This project received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreements no. 284725 and no. 285492. This work reflects only the view of the author and the European Union is not liable for any use that may be made of the information contained therein.

Funded by the
European Union

Researcher declaration to accompany the submission of written work
Department of Law – LL.M. and Ph.D. Programmes

I Maria Grazia Porcedda certify that I am the author of the work "Cybersecurity and Privacy Rights in EU Law. Moving beyond the trade-off model to appraise the role of technology" I have presented for examination for the Ph.D. at the European University Institute. I also certify that this is solely my own original work, other than where I have clearly indicated, in this declaration and in the thesis, that it is the work of others.

I warrant that I have obtained all the permissions required for using any material from other copyrighted publications.

I certify that this work complies with the Code of Ethics in Academic Research issued by the European University Institute (IUE 332/2/10 (CA 297).

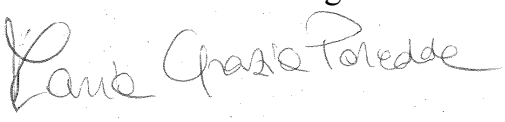
I declare that this work consists of ca. 147000 (pp.1-374, footnotes included) words.

Statement of inclusion of previous work (if applicable):

I confirm that section 2 of the introduction draws upon the thesis I submitted in 2012 to achieve my LLM. I confirm that section 2 of chapter 4 draws upon an earlier article I published in "Lessons from PRISM and Tempora: the self-contradictory nature of the fight against cyberspace crimes. Deep packet inspection as a case study", 25 Jahrgang Seite 305-409, Neue Kriminalpolitik 4/2013, Nomos. I confirm that chapter 5 was the result of previous study for the FP7 SURVEILLE project I undertook at the EUI. I confirm that chapters 6 and 7 draw upon an earlier article I published as "Paper Establishing Classification of Technologies on the Basis of their Intrusiveness into Fundamental Rights", SURVEILLE FP7 Project Deliverable 2.4, April 2013 and as "Report on Regulatory Frameworks concerning Privacy and the Evolution of the Norm of the Right to Privacy" (with Mathias Vermeulen and Martin Scheinin), SurPRISE FP7 Project Deliverable 3.2, February 2013."
Please note that all old work has been updated and substantially changed.

Statement of language correction (if applicable):

This thesis has been corrected for linguistic and stylistic errors. I certify that I have checked and approved all language corrections, and that these have not affected the content of this work. Signature and date: 13 March 2017



ABSTRACT

This thesis concerns a specific instance of the trade-off between security and 'privacy rights', namely cybersecurity, as it applies to EU Law. The research question is whether, and how, the pursuit of cybersecurity can be reconciled with the protection of personal data and respect for private and family life, which I treat as two independent rights. Classic legal argumentation is used to support a normative critique against the trade-off; an in-depth scrutiny of '(cyber)security' and 'privacy' further shows that the trade-off is methodologically flawed: it is an inappropriate intellectual device that offers a biased understanding of the subject matter.

Once the terms of discussion are reappraised, the relationship between cybersecurity and privacy appears more nuanced, and is mediated by elements otherwise overlooked, chiefly technology. If this fatally wounds the over-simplistic trade-off model, and even opens up avenues for integration between privacy and cybersecurity in EU law, on the other hand it also raises new questions.

Looked at from the perspective of applicable law, technology can both protect and infringe privacy rights, which leads to the paradox of the same technology being both permissible and impermissible, resulting in a seeming impasse. I identify the problem as lying in the combination of technology neutrality, the courts' avoidance in pronouncing on matters of technology, and the open-ended understanding of privacy rights.

To appraise whether cybersecurity and privacy rights can be reconciled, I develop a method that bridges the technological and legal understandings of information security and privacy, based on the notions/methods of protection goals, attributes and core/periphery or essence, and which has the advantage of highlighting the independence of the two privacy rights. A trial run of the method discloses aspects of the 'how' question that were buried under the trade-off debate, viz. the re-appropriation of the political and judicial process *vis-à-vis* technology.

TABLE OF CONTENTS

1 LIST OF FIGURES AND TABLES

2 LIST OF ABBREVIATIONS

AFSJ	Area of Freedom, Security and Justice
BEREC	Body of European Regulators for Electronic Communications
CERT	Computer Emergency Response Team
Charter	Charter of Fundamental Rights of the European Union
CFSP	Common Foreign and Security Policy
CIA	Confidentiality, integrity, availability
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CSDP	Commons Security and Defence Policy
CSIRT	Computer Security Incident Response Team
(D)DoS	(Distributed) Denial of Service (attack)
DPI	Deep packet Inspection (also hyphenated)
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECJ	European Court of Justice
eIDAS	Electronic-Identity and Assurance Services
EHRC	Equality and Human Rights Commission
ENISA	European Network and Information Security Agency
EU	European Union
FRA	Fundamental Rights Agency
GCHQ	Government Communications Headquarters (UK)
HRC	Human Rights Committee
HRMF	Human Rights Measurement Framework
ICCPR	International Covenant on Civil and Political Rights
ISO	International Organization for Standardization

ITU	International Telecommunication Union
LEAs	Law Enforcement Agencies
OECD	Organization for Economic Cooperation and Development
OHCHR	Office of the High Commissioner on Human Rights
OSI	Open Systems Interconnection (model)
NGNs	Next Generation Networks
NIS	Network and Information Security
NSA	National Security Agency (US)
PbD	Privacy by Design
PETs	Privacy-enhancing technologies
PIT	Privacy-intrusive technologies
PPP	Public-private partnership
RoL	Rule of Law
R.Q.	Research Question
SIGINT	Signals Intelligence
SurPRISE	Acronym of the project "Surveillance, Privacy and Security"
SURVEILLE	Acronym of the project: Surveillance: ethical issues, legal limitations and efficiency
Telcos	Telecommunication Companies
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
Union	European Union
US	United States

ACKNOWLEDGMENTS

"Il n'y a pas d'efforts inutiles, Sisyphe se faisait des muscles…Il n'y a pas non plus d'errements improductifs. Chacun d'eux accroît l'ouverture d'esprit et la sensibilité de celui qui s'y hasarda."
Paul Valéry and Roger Caillois [1]

"E son di quegli ancora che, più dispettosamente che saviamente parlando, hanno detto che io farei più discretamente a pensare donde io dovessi aver del pane che dietro a queste frasche andarmi pascendo di vento. E certi altri in altra guisa essere state le cose da me raccontatevi che come io le vi porgo s'ingegnano in detrimento della mia fatica di dimostrare."
Giovanni Boccaccio[2]

I warn the reader that these acknowledgments are long, not out of a sense of proportion with the rest of the thesis, but because the people who deserve to be thanked for the support they gave me throughout these years are indeed many.

According to the etiquette of acknowledgments, one should begin with the supervisor. I could not be more pleased to bow to the rules, because this thesis would have not seen the light without the first-class supervision of Professor Marise Cremona.
Marise adopted me, academically speaking, in September 2015, but I wrote the bulk of my thesis under her watch. When I met Marise, I had just given up on the delusion of finding a 'mentor', someone who would see the good in me and help me to hone it. Maybe, like many kids born in the 1980s, I had been swayed by a Hollywoodised misrepresentation of mentorship. Expectations aside, though, you know a mentor when you meet one. This is what Marise has been to me. She has showed me, simply by her example, a gracious way to academia. Marise quietly emanates the virtues of scholarship as a mission: passion for learning, impeccable professionalism, great competence, respect for the interlocutor, and deep humanity. I will never be able to thank her enough for our countless meetings, when she taught me how to master my over-eagerness and learn how to train, Sysiphus-like, the muscles necessary to achieve this PhD. If I will be able to teach and supervise someone successfully, but also know how to defend my work, and myself, I know to whom I will owe this. Thank you, Marise.

I would further like to thank Laurence Duranel, who kindly made all necessary arrangements for the submission of my thesis and the ensuing defence. My gratitude goes also to the members of the jury, Professors Deirdre Curtin, Anne Flanagan and Ronald Leenes, for their time, comments and suggestions, which will help taking this work to the next level.

[1] Paul Valéry, quoted by Roger Caillois, in his *Réponse de M. Roger Caillois au discours de M. Claude Lévi-Strauss. Discours Prononcé dans la Séance Publique le jeudi 27 juin 1974 Paris Palais de l'institut*. The second and third sentences are by Roger Caillois himself. In English (translation mine): "There are no useless efforts, Sysiphus was training his muscles…Neither are there improductive endeavours. Each of them deepens the open-mindedness and sensitivity of the person attempting them".
[2] Giovanni Boccaccio, 'Quarta Giornata, Introduzione', in *Decameron* (1350 ca.). "Those again there are, who, evincing less wisdom than despite, have told me that I should shew sounder sense if I bethought me how to get my daily bread, than, going after these idle toys, to nourish myself upon the wind; while certain others, in disparagement of my work, strive might and main to make it appear that the matters which I relate fell out otherwise than as I set them forth" (source: https://en.wikisource.org/wiki/The_Decameron/Novel_4,_1).

Before my encounter with Marise, I wore the double hat of PhD researcher and research associate in two EU-funded research projects, SurPRISE and SURVEILLE. During that intense time, which, I must acknowledge, I could have not experienced if Prof. Martin Scheinin had not given me a second chance at the EUI, I gained amazing experience and met extraordinary people.
I would like to especially thank Dilini, Emma, Jacob, Jaro, Johann, Marta, Nanna, Regina, Reinhard, Stefan and Walter, all colleagues within the SurPRISE project, for their support and encouragement in the early stages of my career.
A warm thanks to Melissa, who gave me crucial practical and emotional support in juggling the organization of the large-scale participatory event with the submission of the two-thirds of my thesis. Melissa, you have been a great colleague and friend.
I met lovely people also through the SURVEILLE project. First of all Jonathan, with whom I have shared all the joy, pain and mould of the projects' den in Casale! Thank you for having been a good friend and, more than once, a guide. I hope I could teach you as much as you have taught me. The memory of the delicacies from projects' trips we shared in the office, and the pride of our common fight, will stay with me for good.
Then Elisa, who, with energy and skilfulness, seized the chance and turned the FP7 project into an opportunity. Working with you and Sebastian on our edited book was a balm to my soul. I do hope this is only the beginning of a longer-term collaboration, and friendship.
I must also mention Jens, for the many pleasant project lunches and dinners, and chats on a common (academic) passion, cybercrime.
Life during the projects was also made enjoyable by 'the girls', Federica, Karolina, Madalina and Nicole (most of whom were also lovely colleagues in CharterClick! project), who many a times solaced my grump with a friendly chat, their kind heart and a piece of chocolate. The same did Alessandro, Andrea, Antonella, Laura and Simona, as well as Cinzia, Paola and Antonella.

Some of the people who deserve a mention came across my path as a result of those "*errements improductifs*" praised by Caillois. Thanks to Alina, Federica, Karolina, Maria Luisa and Paula for the great work we have done together to improve the working conditions of research associates. My mind and sensitivity have certainly gained from getting to know you and striving toward a shared goal. As a result of both the "*errement improductif*", and those attitudes so aptly summarized by Boccaccio, I met Agnes, Fatma, Veerle and Xenia. Thank you for having taken the time to listen, and for having offered relief and precious advice.

Thanks also to Mariangela, a doctor by vocation, who read my soul and introduced me to the charity *Gli Amici di Daniele*, which helps people avoiding what happened to Alba's son, who committed suicide following bullying in the workplace. Thanks to Alba's courage, to Mariangela, Nunzia, and other volunteers who run the helpdesk, I recovered my confidence and the energy to finish my work.
My sincere gratitude also to Alfonso and Bénédicte, who walked me through the exit of *inferno*, and Claudia Carraresi, who taught me how to check –and recognize– myself in the mirror.

Other colleagues, met through or thanks to the EUI, deserve my gratitude for having encouraged me to keep pursuing my research: Patryk Pawlak, Helena Farrand Carrapico, Giovanni Sartor, Paolo Gentile and Giampiero Giacomello. Thank you all.

There is more to the EUI than work: through it I met wonderful people. Thanks to the companions of many lunches, coffees and dinners: Alexandra, Anna&Rob, Benedetta, Emma, Emmanuelle, François, Giuliana, Inés, Janine, Kasia, Matt, Nina, Payam, Raphael, Serena, and Trond. My warmest thanks to those who shared it all –a pouffe-bed, work&leisure, Christmas, trips, long phone calls, holidays, tears and joy: Claire&John, Federica, Karolina, Jonathan, Mathias (Möschel), Madalina&Tudor and Trajche.

Friends from Spanish deserve a separate paragraph, to stand out as much as a class that reflects the incredible qualities of its animator and dear friend, Edurne. If I could rate the activities of the EUI, this would be my favourite by far. *Gracias a todas y todos los que han compartido conmigo años maravillosos de charlas, bromas, gramática, veladas, historias (muy privadas) y, sobre todo, felicidad. Gracias a Anna, Bruno, Evy, Krzys, Ivana, Laura, Lorenzo, Ognjen, Ricardo, Sabrina y Silvia, y otros que conocí antes, como Sabrina. Os echaré de menos. Gracias Edurne, eres única.*

Thanks also to Mara, Valerio, and Marco, for making me still love dancing, teaching me how to sing, and not losing faith with my swimming!

Genuine thanks to the great friends I met through my peregrinations before and outside of the EUI. *Grazie alle mie tesore, Cinzia, Elisa, Gloria, Ilaria, Lucia e Melissa (ma sì, anche Bronco!), per esserci sempre. Grazie anche a te Valentina, lontana ma sempre vicina. Merci Bénédicte pour toutes interactions rigolotes, tous voyages, ton aide quand j'ai en vraiment eu besoin, et ton amitié sans fine*. Thanks to Lukas for the brilliant Skype calls, which make me feel like no time has passed since our Erasmus in Nottingham. Thanks to Francesca, and Rod&Rachel.
My warm gratitude to people that I met in a distant past, and are still my friends. *Grazie Anna Maria, Federica, Francesco, Gianluca, Bruna e Gigi.*

Thanks to many members of my family, they are the most fabulous supporters. *Grazie di cuore a Mary e Zia Grazia per il sostegno incondizionato. Grazie a Chiara, e Ilaria, che affrontano il mare pur di esserci. Grazie a Esteban, che il mare non riuscirà a solcarlo, ma che c'è col cuore, assieme a Marta, Alessandro e Sofia*.
A very special thank to Audrey and Les, who are to me like another pair of loving (and lovely) parents.
Thanks to mum and dad, who are always there, no questions asked. *Mamma e babbo, grazie. Mi ha commosso quando mi avete detto che questo dottorato vi rende orgogliosi di me, non potrò dimenticarmelo, così come tutto il sostegno morale, emotivo e materiale che mi avete dato nell'ultimo anno per poterlo portare a compimento. Vi voglio bene.*

My last and most passionate acknowledgment goes to Martyn, meeting whom was one of the two strokes of serendipity in Florence and the EUI. You have been here for me, with your love, all along, like (you say) I have been for you. This thesis is dedicated to you, like yours to mine, because we have done this together.

I had come to Florence and the EUI with clear ideas in mind: to grow academically, learn how to swim and drive, and to pick up another language. Out of hard work and good luck, those wishes came true. The other stroke of serendipity was the unintended result of all the encounters, fatigue, mixed endeavours, and obstacles placed on my path. Here, in Florence and the EUI, I have discovered my strengths and weaknesses, and learnt how to love them all, and with that, how to have faith in myself. I could have not asked for more.

INTRODUCTION

R.Q.: Can the rights to respect for private and family life and the protection of personal data be reconciled with the pursuit of cyber-security, as defined in the European Union? If so, how [can they be reconciled], taking into consideration technological constraints?

This question is a policy-relevant specification of the broader theoretical debate on trading-off liberties with security, and particularly 'security v. privacy'. I began meditating on the puzzle six years ago, when I was working on access by law enforcement agents to data stored in the cloud. This was before Edward Snowden made his revelations, which seemingly destabilized the trade-off model, and also before the recrudescence of terrorism in Europe, which brought firmly (and sadly) back in fashion the conundrum of 'security v. privacy'. Logically, the policy responses to these events have changed the field and necessarily shaped my approach to the question, not least because, in the early drafting stages of this work, I was a member of two research consortia focussing on the European Union's policy on security and liberty (*infra*, section 4.1).

Partly as a result of these factors, this introduction is structured as follows. In section one I situate my research question against the backdrop of both the Snowden revelations and the recrudescence of terrorism in Europe. In section two I break down the research question into sub-units and corresponding hypotheses, from which I illustrate the broader plan of the thesis (section three). Finally, in section four I clarify the scope of the research and its relationship with the FP7 research projects SurPRISE and SURVEILLE.

1 SITUATING THE RESEARCH QUESTION: THE TRADE-OFF MODEL AND THE SNOWDEN REVELATIONS

In this section I introduce the two macro policy topics that set the backdrop for my research question, i.e., the trade-off model ensuing from counterterrorism, and the Snowden revelations. In the first subsection (1.1) I provide a synopsis of the trade-off argument within counterterrorism, where I also anticipate my normative position. I then (section 1.2) introduce security v. privacy with reference to the exceptional access and mass surveillance programs revealed by Snowden. Based on Snowden's revelations I elaborate three reflections that help to introduce the case study (section 1.3).

1.2 THE TRADE-OFF MODEL AS A HALLMARK OF COUNTERTERRORISM

The attack on the World Trade Centre in New York marked the beginning of a 'long decade'[3] of policy responses to terrorist attacks perpetrated by violently radicalized Muslims. Following 9/11, the list of attacks has sadly continued to grow, forming a macabre account.[4] After each attack, a typical reaction has consisted in governments on both sides of the Atlantic declaring a state of emergency, if not of war, and demanding to be given the widest possible powers to apprehend those responsible for spreading terror. Policy responses have targeted critical infrastructure (particularly airports or points of entry), stiffened criminal law provisions, and even paved the way to military action. Such measures, which have been amply commented upon in the literature,[5] typically require the 'temporary' compression of

[3] David Jenkins, 'Introduction. The Long Decade' in David Jenkins, Amanda Jacobsen and Anders Henrikens (eds), *The long decade. How 9/11 changed the law* (Oxford University Press 2014).

[4] For a non-exhaustive list, see The 9/11 Commission, 'Final Report of the National Commission on Terrorist Attacks Upon the United States', New York, (2004); Congreso de los Diputados, *Comisiones de Investigacíon sobre el 11 de marzo de 2004, Diario de Sesiones n° 24* (Cortes Generales, 2005); United Kingdom, Home Office, *Report of the Official Account of the Bombings in London on 7th July 2005* (House of Commons, 2006). The Ram Pradhan Inquiry Commission was published by Sunil Ghume, 'Senior Officers don't Even Look at Intelligence Reports: 26/11 Panel' *The Times of India* (2 December); M. George Fenech and M. Sébastien Pietrasanta, *Rapport fait au Nom de la Commission d'Enquete Relative aux Moyens mis en œuvre par l'État pour Lutter Contre le Terrorisme Depuis le 7 janvier 2015* (Assemblé Nationale, 2016).

[5] For measures adopted in the United States, see Laura K. Donohue, *The Cost of Counterterrorism. Power, Politics and Liberty* (Cambridge University Press 2008); Bruce Ackerman, *Before the Next Attack. Preserving*

the enjoyment of liberties, which are seen as hindering the pursuit of security. In other words, the threat to security is typically deemed so fundamental (i.e. it is securitized[6]) as to justify the limitation of liberties beyond levels previously considered permissible. This is, in short, the security v. liberty argument, the most relevant of which is Posner and Vermeule's trade-off model (chapter 1). The range of affected fundamental rights[7] is broad, and includes dignity, non-discrimination, the prohibition of torture and inhuman or degrading treatment, the right to liberty and security, the right to the protection of personal data (a.k.a. information or data privacy), the right to respect for private and family life (a.k.a. privacy), freedom of thought, conscience and religion, freedom of expression and information, freedom of assembly and of association, freedom of movement and residence, the right to an effective remedy and to a fair trial, the presumption of innocence and right of defence, etc.

The premise of this work is that the European Union (hereafter the Union or EU) should reject the trade-off model, which I consider a fallacious, value-laden political choice "claiming the mantle of legality",[8] or rule *by* law[9] (as opposed to rule *of* law). To be sure, this argument does not rest on a normative opposition between the EU and the US. As I will discuss in chapters 1 and 2, my challenge to the trade-off can be exported, but my arguments focus on the Union as the jurisdiction of reference of this study. Alongside the trade-off, Union law should reject the trade-off's nefarious consequences, such as lopsided balancing,[10]

Civil Liberties in an Age of Terrorism. (Yale University Press 2006); Amitai Etzioni, *How Patriotic is the Patriot Act* (Routledge 2004); Stephen J. Schullhofer, *Rethinking the Patriot Act. Keeping America Safe and Free* (A Century Foundation Report, 2005); R.P. Abele, *A Users' Guide to the USA Patriot Act and Beyond* (University Press of America 2005); Daniel Solove, *Nothing to Hide: the False Trade-off Between Privacy and Security* (Yale University Press 2011). For the European Union, see David Anderson, *The Terrorism Acts in 2011. Report of the Independent Reviewer on the Operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006* (Parliament, The Stationery Office 2012); Kate Moss, *Balancing Liberty and Security. Human Rights, Human Wrongs* (Palgrave Macmillan 2011); Francesca Galli and Anne Weyembergh (eds), *EU Counter-terrorism Offences. What Impact on National Legislation and Case Law?* (Editions de l'Université de Bruxelles 2012); Stefano Rodotà, *Intervista su Privacy e Libertà. A cura di Paolo Conti* (2005). At the international level, see Martin Scheinin, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, A/HRC/13/37* (2009); Martin Scheinin and Mathias Vermeulen, 'Unilateral Exceptions to International Law: Systematic Legal Analysis and Critique of Doctrines to Deny or Reduce the Applicability of Human Rights Norms in the Fight against Terrorism' (2011) 8 Essex Human Rights Review 20-56. For a more general reflection on the effects of harsh security policies, see Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, (2003); Tony Monahan, *Surveillance and Security. Technological Politics and Power in Everyday Life*, (2006); Michael Levi and David S. Wall, 'Technology, Security and Privacy in Post-9/11 European Information Society' (2004) 31 Journal of Law and Society.

[6] Barry Buzan, Ole Weaver and Jaap De Wilde, *Security: a New Framework for Analysis* (Lynne Rienner 1998).

[7] The document of reference is the Charter of Fundamental Rights of the European Union, OJ C 303/01.

[8] David Dyzenhaus, 'States of Emergency' in Michel Rosenfeld and András Sajó (eds), *The Oxford Handbook of Comparative Constitutional Law* (Oxford Handbooks Online 2012), p. 451.

[9] Jenkins (2014).

[10] Martin Scheinin, *Terrorism and the Pull of 'Balancing' in the Name of Security. Law and Security, Facing the Dilemmas* (European University Institute Law Working Paper 11, 2009).

profiling, the expansion of the scope of criminal law, and the normalization of the state of exception.

The latter is one of the major issues after 9/11: since the fight against terrorism is open-ended, so are the counterterrorism measures enacted. [11] When David Jenkins[12] asked whether Snowden's revelations on mass surveillance could chase away the danger of normalizing the exceptional measures adopted, or on the contrary open the horizon to a dystopian world, the Islamic State in Iraq and the Levant (ISIL or Da'esh) had just made its appearance, and the deadly multiple attacks of 2015 were still to come. The tangible possibility that we will end up talking about 'long decade*s*' of normalized emergency legislation makes a discussion of the relationship between security and liberties compelling. This includes 'security v. privacy', to which I turn now.

1.2 SECURITY V. PRIVACY: EXCEPTIONAL ACCESS AND THE SNOWDEN REVELATIONS

'Security versus privacy' constitutes a classical version of the trade-off model, since traditional telecommunications as well as computers and their networks can generate the evidence necessary to apprehend terrorists and their aiders (chapter 2). In fact, after 9/11 politicians have tried to make the case for obtaining investigatory powers that are as wide as possible. Alongside demanding telecommunications companies to retain data concerning the use of telecommunications by their customers, which in the Union led to the invalidated data retention Directive (chapter 1), governments vouched for sweeping powers of interception not matched by adequate safeguards, not least sunset clauses.

Following the wave of terrorism in 2015, demands of powers of interception have concerned activities online, or in cyberspace (chapter 3). This is due to the – trite – fact that we live in an information society benefitting everyone, law-abiding citizens as well as criminals. As a global repository of information and a popular avenue for exchange, the

[11] Katija Sugman Stubbs and Francesca Galli, 'Inchoate Offences.The Sanctioning of an Act Prior to and Irrespective of the Commission of any Harm' in Francesca Galli and Anne Weyembergh (eds), *EU counter-terrorism offences. What impact on national legislation and case law?* (Editions de l'Université de Bruxelles 2012).
[12] Jenkins (2014).

Internet offers would-be terrorists propaganda, information on how to manufacture explosive devices, how to affiliate to the extremist group of choice, interact with like-minded people and arrange terrorist acts.[13] Such facts have become the object of inchoate crimes (chapter 1) featuring in proposed legislation.[14]

The availability of secure transactions based on encryption, which has enabled the Internet boom and is encouraged to sustain its economy,[15] represents an investigatory hurdle[16] that politicians are trying to remove. Echoing the crypto wars of two decades ago, recently politicians on both sides of the Atlantic have raised anew the desire that technology vendors embed in their products "exceptional access", [17] i.e. the capability of decrypting data contained in computers (devices) and information systems by default. The request is troubling in many respects, but also puzzling since, as the 'IPhone case' has shown,[18] human ingenuity can overcome technological hurdles when needed. The impact on privacy rights of such requests should be apparent.

Pleas for (lawful) exceptional access come only three years after a global consortium of newspapers reported the revelations of Edward Snowden concerning mass-scale surveillance programs, such as Tempora[19] and Prism,[20] led by the UK and US with the cooperation of allied governments, including many members of the Union.[21] Although the reconstruction of the surveillance programs offered by newspapers was not always the most accurate or

---

[13] United Nations, Office on Drug and Crime (UNODC), *The Use of Internet for Terrorist Purposes* (2012).

[14] European Commission, *Proposal for a Directive on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism* ((Communication) COM (2015) 625 final, 2015).

[15] European Commission, *A Digital Single Market Strategy for Europe* ((Communication) COM (2015) 192 final, 2015).

[16] Fabio Tonacci, 'Terrorismo, la Rete Criptata: così la Cyber-jihad Comunica con i Lupi Solitari in Europa' *La Repubblica* (26 July 2016).

[17] Harold Abelson and others, 'Keys under doormats: mandating insecurity by requiring government access to all data and communications' (2015) 0 Journal of Cybersecurity 1-11. The article refers to requests by the US and UK governments; the French and German ministers of home affairs have recently expressed similar desires. Ministère de l'Intérieur français, *Initiative Franco-allemande sur la Sécurité Intérieure en Europe* (Retrieved on EDRi-gram newsletter 14.16, 24 August 2016) <http://www.interieur.gouv.fr/Le-ministre/Interventions-du-ministre/Initiative-franco-allemande-sur-la-securite-interieure-en-Europe>.

[18] Susan Landau, 'The Real Security Issues of the iPhone Case' (2016) 352 Science 1398-1399. There, she urges the FBI to develop better capabilities as part of the 'Going Dark' programme, which deals with lawful hacking (which the FBI has been engaged in since 2003).

[19] Ewen MacAskill and others, 'GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications' *The Guardian* (21 June 2013).

[20] Barton Gellman and Laura Poitras, 'Documents: U.S. Mining Data from 9 Leading Internet Firms; Companies Deny Knowledge' *Washington Post* (6 June 2013); Glenn Greenwald and Ewen MacAskill, 'NSA Taps in to Systems of Google, Facebook, Apple and Others, Secret Files Reveal' *The Guardian* (7 June 2013).

[21] Nils Muižnieks, 'Human Rights at Risk When Secret Surveillance Spreads' (*The Council of Europe Commissioner's Human Rights Comment*, 24 October 2013) <https://www.coe.int/en/web/commissioner/-/human-rights-at-risk-when-secret-surveillance-sprea-1> accessed 16 August 2016.

complete,[22] the substance of the revelations was not contested by the responsible authorities.[23] The disclosed schemes consist in an evolution of previous programs, such as ECHELON[24] (now FORNSAT[25]) based on "far-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner".[26]

Under the cloak of national security[27] concerns – hiding economic and political espionage,[28] profiling on political grounds[29] as well as standard policing – huge proportions of global communications can be potentially submitted to the listening and retaining powers of intelligence services without legal basis,[30] warrant and oversight.[31] For instance, the NSA and GCHQ dispose(d) of wide instruments to collect information produced by telephone and electronic communications, such as "tapping fibre-optic cables, circumventing encryption,[32]

---

[22] For a reconstruction of the programs and the technology involved, see Michelle Cayford, *Paper on Mass Surveillance by the National Security Agency (NSA) of the United States of America* (Extract from SURVEILLE Project Deliverable D 2.8 2014). I wrote about the potential use of deep packet inspection in Maria Grazia Porcedda, 'Lessons from PRISM and Tempora: the Self-contradictory Nature of the Fight against Cyberspace Crimes. Deep packet Inspection as a Case Study' (2013) 25 Neue Kriminalpolitik 305-409.

[23] European Parliament, *Resolution on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs* (2013/2188 (INI), 2014), point I.

[24] A global system for intercepting communications operated by the United States, the United Kingdom, Canada, Australia and New Zealand under the UK-USA Agreement, European Parliament, LIBE Secretariat, *Background Note. The European Parliament's temporary committee on the ECHELON interception system* (2014).

[25] European Parliament, 'Interception Capabilities 2014' (2014) <http://www.europarl.europa.eu/document/activities/cont/201309/20130916ATT71388/20130916ATT71388EN.pdf>.

[26] European Parliament (2014), *Resolution on the US NSA Surveillance Programme*, point 1.

[27] Article 29 Data Protection Working Party, *Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes* (819/14/EN WP 215, 2014).

[28] Muižnieks (2013).

[29] European Parliament (2014), *Resolution on the US NSA Surveillance Programme*, recital G.

[30] To be entirely sure, a blurred legal basis may be retrieved in article 32 of the Cybercrime Convention (chapter 3), which enables contracting states to collect open source evidence or obtain it from the controller of information with his or her consent, hence bypassing existing mutual legal assistance treaties or mechanisms. Indeed, Snowden disclosed deep and long-standing relationships between the NSA and major service providers. Greenwald and MacAskill (2013). In its resolution, the EP has voiced serious criticism in relation to talks about further expanding article 32 of the Cybercrime Convention. European Parliament (2014), *Resolution on the US NSA Surveillance Programme*, points 33 and 36.

[31] For a discussion of the supervision under which the intelligence services of EU countries operate, see Article 29 Data Protection Working Party (2014); Fundamental Rights Agency, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Mapping Member States' legal frameworks* (Publications Office of the European Union, 2015).

[32] Or intercepting data detained by major US cloud providers in transit unencrypted from their EU data centres to the US. European Parliament, *LIBE Committee Inquiry on the Electronic Mass Surveillance of EU Citizens: Protecting Fundamental Rights in a Digital Age. Proceedings, Outcome and Background Documents* (2014).

launching cyber attacks,[33] gathering phone metadata, and utilizing traditional spying methods such as bugging embassies and tapping political leaders' phones."[34]

As far as the United States is concerned, the NSA can build databases and retain the data for 5 years or longer, with very weak limitations. The collection could entail seemingly anyone, irrespective of any grounds of suspicion in relation to (serious) crime. In fact, the widely debated distinction between non-United States persons and unconsenting United States citizens – whereby foreign intelligence could be collected almost unlimitedly for the former, but not for the latter – could be removed if matching a wide number of exceptions,[35] and in any case by the will of the NSA director.

In the next sections I reflect on three implications of such mass-scale surveillance – an epitome of the trade-off model extended to 'cyberspace'– that help introduce the case study and frame the research question.

1.3 THREE REFLECTIONS STEMMING FROM THE SNOWDEN REVELATIONS

The first reflection (section 1.3.1) is that both exceptional access and mass-scale surveillance programs are an epitome of the trade-off logic, which forces us to reflect on the fact that data are evidence. Secondly (section 1.3.2), Snowden's revelations sparked a debate which challenges the trade-off logic, reminding us that the EU's *ordre public* aims at reconciling security with privacy, not the opposite; this means finding an adequate solution for the protection of data, and the fact that (cyber)crime-related evidence requires data. Finally, Snowden's revelations show that the application of the trade-off logic to cyberspace may backfire, thus urging reconciliation and making security online a particularly interesting case study for the trade-off model.

[33] Such as against Belgacom, the telecommunications company contracted by Union institutions. Ibid, point 90.
[34] Cayford (2014), p. 30.
[35] Detailed in Section 5 on Domestic Communications of the Secret/COMINT/NOFORN/20320108, made available by Glenn Greenwald and James Ball, 'Revealed: the Top Secret Rules that Allow NSA to Use US Data without a Warrant' *The Guardian* (20 June 2013).

1.3.1 MASS SURVEILLANCE FOLLOWS THE TRADE-OFF: DATA AND COMMUNICATIONS AS EVIDENCE

First, the revelations testify to the blurred line between intelligence and policing (see chapter 1) denounced by both parliamentary assemblies of the Council of Europe and the EU in their respective resolutions.[36] Signal intelligence, or SIGINT, has evolved from an instrument of targeted espionage and external intelligence to one of strategic, proactive surveillance of ordinary telecommunications, also for internal policing, whose arsenal and remit expands as Internet applications grow.[37] In its resolution on the NSA revelations, the European Parliament denounced [38] the NSA purchasing campaign of 'zero-day' exploits, i.e. crucial vulnerabilities in software, unknown by vendors and users, that expose machines to serious attacks. Such activities, recently confirmed by the information security community,[39] had been discussed for years in expert circles,[40] alongside their heavy implications for network and information security (and ability to backfire,[41] enabling cybercrime) and privacy rights.

Yet, from the perspective of agencies using these systems, such implications are minor, in that 'cyberspace' is seen as a source of intelligence/evidence or, at most, as a medium for (cyber)crime, rather than something to defend – apart from against the prying eyes of economic and political competitors. As a result, data are the object of collection, and communications are something to monitor, not to protect. This is a full trade-off perspective, where privacy rights are seen as an investigatory hurdle to be overcome (or balanced) due to superior 'national security' concerns justifying secrecy and action above constitutional law. Requests for 'exceptional access' also fall under this logic.

---

[36] European Parliament (2014), *Resolution on the US NSA Surveillance Programme*; Council of Europe, Parliamentary Assembly, *Resolution 2045 (2015) on Mass Surveillance* (2015).

[37] Council of Europe, Venice Commission, *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on Democratic Oversight of Signals Intelligence Agencies* (CDL-AD(2015)006, Study n. 719/2013, 2015).

[38] European Parliament (2014), *Resolution on the US NSA Surveillance Programme*, point BS.

[39] Bruce Schneier, 'The NSA is Hoarding Vulnerabilities' (*CRYPTO-GRAM September 15*, 2016) <https://www.schneier.com/crypto-gram/archives/2016/0915.htm> accessed 15 September 2016.

[40] Lilian Edwards, Ian Brown and Christopher Marsden, 'Information Security and Cybercrime' in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet (3rd edition)* (Hart 2009). In their chapter, they describe four different markets for zero-day exploits, one being governmental agencies such as the NSA.

[41] Recent news reports revealed an auction of a trove of zero-day exploits hacked from the NSA possibly by Russian groups. Andy Greenberg, 'The Shadow Broker Mess is What Happens When the NSA Hoards Zero-days' *Wired* (17 August 2016).

In point 16 of its resolution, the EP criticized reliance on the national exemption clause,[42] and explicitly mentioned the case of *ZZ*, where the Court of Justice of the European Union (hereafter CJEU) stated that "although it is for Member States to take the appropriate measures to ensure their internal and external security, the mere fact that a decision concerns State security cannot result in European Union law being inapplicable."[43] The EP has also recalled states' obligations under the ECHR.

1.3.2 THE SNOWDEN REVELATIONS SPARKED THE NEED TO OVERCOME THE TRADE-OFF

The point remains, however, that personal data and communications represent a source of evidence, and that a *modus vivendi* must be found to accommodate fundamental rights and investigatory needs. Hence, and secondly, the revelations remind us that security and liberty can be reconciled by restoring the rule of law.

On the one hand, it was proposed to constrain intelligence services at the national level,[44] possibly creating a supra-national oversight agency.[45] Oversight would also play in favour of efficiency, since testimony has revealed that the mass-surveillance programs resulted in preventing zero terrorist attacks and diverted funds from other, more efficient efforts and technology.[46]

On the other hand, the revelations revived the discussion on the importance of privacy rights[47] to democracy.[48] The adopted resolutions demand a stringent protection of such

[42] Which it openly challenges in point 37, when it considers that "large-scale access by US intelligence agencies to EU personal data processed by Safe Harbour does not meet the criteria for derogation under 'national security'" European Parliament (2014), *Inquiry on the Electronic Mass Surveillance of EU Citizens*.
[43] Judgment of 4 June 2013 in ZZ, C-300/11, EU:C:2013:363, para 38. Pronounced to support the admissibility of the case.
[44] Fundamental Rights Agency (2015).
[45] European Parliament (2014), *Resolution on the US NSA Surveillance Programme*.
[46] Ibid, recital O.
[47] On the violation of privacy from the perspective of international law, see European Parliament, LIBE Committee, *Statement by Professor Martin Scheinin* (Hearing within the Inquiry on Electronic Mass Surveillance of EU Citizens, 2013).
[48] Laura K. Donohue, 'NSA Surveillance May Be Legal — but it's Unconstitutional' *The Washington Post* (21 June 2013); European Digital Rights (EDRI), *US Agencies Have Unlimited Access to Internet Data* (EDRI-gram newsletter, n. 11.12 2013); Jill Lepore, 'The PRISM. Privacy in an Age of Publicity' *The New Yorker* (24 June 2013); Karlin Lillington, 'It's Good to Talk in Public about Privacy and Data Protection' *Irishtimes.com* (19 June 2013).

rights,[49] to the effect that "information flows and data, which today dominate everyday life and are part of any person's integrity, need to be as secure from intrusion as private homes."[50] Although the recrudescence of terrorism in 2015-2016 has moved public attention away from the subject matter, debates continue in courts, e.g. with the much awaited proceedings of the case filed by Big Brother Watch and Others pending before the ECtHR.[51] From this perspective, the secret incursions in 'cyberspace' represent an undue subversion of the paradigm whereby security should serve the enjoyment of rights, and risk subverting democracy in the name of defending it.

1.3.3 OVERCOMING THE TRADE-OFF MAY PLAY IN FAVOUR OF SECURITY ONLINE

The third and last reflection goes beyond the need to harmonize the needs of investigations with those of fundamental rights. It concerns a point which, although not featuring highly in public debates, surfaced through the parliaments of the CoE and the EP, viz. the attention to security in cyberspace and technological matters.

The parliamentary Assembly of the CoE recommended that Member States ensure "protection of privacy in the digital age and internet safety" as well as "further exploring Internet security issues related to mass surveillance and intrusion practices, in particular with regard to the human rights".[52] But it also expressed deep worries "about threats to Internet security by the practices of certain intelligence agencies… of seeking out systematically, using and even creating "back doors" and other weaknesses in security standards and implementation that could easily be exploited by terrorists and cyberterrorists or other criminals,"[53] such as the 'zero-day exploits' and cyber-offences mentioned above. To this effect it called for promoting "the further development of user-friendly (automatic) data protection techniques capable of countering mass surveillance and any other threats to

[49] United Nations, General Assembly, *Resolution the right to Privacy in the Digital Age, A/RES/68/167* (2013). Council of Europe (2015); Parliamentary Assembly of the Council of Europe, *Recommendation 2067 (2015) on Mass Surveillance* (2015); Committee of Ministers of the Council of Europe, *Reply of the Committee of Ministers to Parliamentary Assembly Recommendation 2067 (2015) on Mass Surveillance* (CM/AS(2015)Rec2067-final, 2015); European Parliament (2014), *Resolution on the US NSA Surveillance Programme*.
[50] European Parliament (2014), *Resolution on the US NSA Surveillance Programme*, recital B.
[51] Big Brother Watch and others, *Joint Application under Article 34* (n 58170/13, 2013).
[52] Council of Europe (2015), points 2.1 and 2.2.
[53] Council of Europe (2015), point 5.

Internet security, including those posed by non-State actors."[54] It then referred to the EP's "call to promote the wide use of encryption…resist any attempts to weaken Internet safety standards, not only in the interest of privacy, but also in the interest of threats against national security posed by rogue States, terrorists, cyberterrorists and ordinary criminals."[55]

Indeed, after noting that "there is no guarantee, either for EU public institutions or for citizens, that their IT security or privacy can be protected from attacks by well-equipped intruders ('no 100 % IT security')" the EP notes that "in order to achieve maximum IT security, Europeans need to be willing to dedicate sufficient resources, both human and financial, to preserving Europe's independence and self-reliance in the field of IT."[56] For the sake of resisting criminal as well as state-sponsored cyber-attacks, the EP made several recommendations[57] concerning the security of 'cyberspace' and its complementarity with the protection of privacy rights. It supports the EU cyber strategy and recommends boosting the development of intra-EU IT capacity and security in software, hardware, cryptography and services (also through specific funding via H2020), to develop EU security and privacy standards, and to incentivise their adoption by manufacturers through appropriate legislation. To increase the transparency and reliability of IT systems, the EP calls for introducing open source software and hardware, also for public procurement purposes, and to impose the adoption of adequate security standards on Telecommunications companies, including end-to-end encryption of their services. It recommends banning the use of backdoors by LEAs, as well as preventing projects that wish to enable illegal access to IT systems from gaining access to H2020 funds. At the EU institutional level, it recommends establishing a Computer Emergency Response Team (hereafter CERT) at ENISA, as well as checking EU institutions' security standards and dependability, and the use of default encryption standards. Last but not least, it recommends introducing an EU routing system, including the processing of call detail records as a substructure of the Internet, and to process records in accordance with the EU legal framework.

The resolution clarifies that state-sponsored surveillance on grounds of national security imperils the security of cyberspace, or cybersecurity, on which such surveillance was based,[58]

---

[54] Ibid, point 19.15.
[55] Ibid, point 17.12.
[56] European Parliament (2014), *Resolution on the US NSA Surveillance Programme*, point 15.
[57] Ibid, points 90-110.
[58] On the subject matter, see, well before the revelations but thematically very close to the subject-matter, Withfield Diffie and Susan Landau, 'Internet Eavesdropping: A Brave New World of Wiretapping' (2008) 299

and proposes the adoption of complementary actions for cybersecurity and privacy. Incidentally, it argues that the programs disclosed by Snowden cannot benefit from any national security exemption precisely because they concern the privacy of EU citizens, as well as the security and reliability of all EU communication networks, which are *in toto* EU law competence.[59] In other words, by putting at risk privacy rights (through enabling surveillance capabilities) for short-term security gains, intelligence services put at a greater risk long-term cybersecurity.

***

In sum, security in cyberspace seems Janus-faced (chapter 3): a venue for collecting intelligence, launching state-sponsored attacks or countering crime, where privacy rights represent the major obstacle, and on the other hand, a 'space' to protect, because of our reliance on networks and information systems for critical infrastructure, including our communications and activities, for which privacy rights and security objectives seem to converge. This is also reflected in the Venice Commission reports, which view SIGINT as an offensive tool, and 'cyber-security' as a defensive tool.[60] Hence, security in cyberspace, or cybersecurity, appears to be a particularly interesting case study to appraise the effects of opposing security and privacy rights and the desirability of their reconciliation.

2 THE RESEARCH QUESTION, HYPOTHESES AND METHODOLOGY

R.Q.: Can the rights to respect for private and family life and the protection of personal data be reconciled with the pursuit of cyber-security as defined in the European Union? If so, how [can they be reconciled], taking into consideration technological constraints?

The R.Q. rests on two assumptions. The first, anticipated in section 1.1 above, is that the trade-off model is normatively wrong; my normative assumption is specific to the Union, but

Scientific American Magazine 4; Susan Landau, *Surveillance or Security? The Risk Posed by New Wiretapping Technologies* (the MIT Press 2010).

[59] European Parliament (2014), *Resolution on the US NSA Surveillance Programme*, point 16.

[60] Council of Europe (2015), para 72.

the argument could be made for other jurisdictions (so as not to imply any 'superiority' of the EU). The second is that cybersecurity is not coterminous with cybercrime, which encompasses at least (chapter 3) two different notions: narrow or online crimes (crimes against data and machines) and broad or off-line crimes (crimes against the person). These 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, and the rules pertaining to its use and exchange. As a corollary, only narrow cybercrime pertains to network and information security, or NIS (which has strong connections with the protection of critical information infrastructure). Based on such assumptions, I advance the following four hypotheses in relation to the R.Q.:

Hypothesis (I): the trade-off model is not an adequate intellectual device to appraise the relationship between security and rights, notably privacy rights.

Hypothesis (II): there can be complementarity between cybersecurity understood as narrow cybercrime/NIS and privacy rights. Complementarity can be of three kinds:

a) Overlap (strong): there is complete overlap between the objectives. The object and means of protection coincide.
b) Convergence (weak): there is a convergence of objectives between cybersecurity understood as narrow cybercrime/NIS and privacy rights.
c) Causality (Intermediate): one sets of rules has a causal positive effect on the other. In other words, 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 and maintain NIS; OR rules adopted pursuant to cybersecurity understood as narrow cybercrime/NIS can act as a proxy to protect privacy rights.

Hypothesis (III): in the case of broad cybercrimes, and in general when 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. This hypothesis also includes two options:

a) Absence of tension between rules (agnosticism): the pursuit of an investigation does not affect privacy rights. This may be the case of narrow cybercrime or NIS, where minimal conflict between privacy and 'security' could pave the way to reconciliation without balancing.
b) Permissibility: the pursuit of an investigation affects privacy rights, but in a way that is permissible, i.e. that does not impair the essence of the rights. This may be the case with broad cybercrimes. Balancing can be avoided by 'early warning'

technology assessment, the core/periphery formula, as well as the design of better procedural rules.

Hypothesis (IV): hypotheses II and III cannot be demonstrated by means of classic legal analysis, due to the combined effect of the paradigm of technology neutrality that affects both law-making and judgments, as well as courts' avoidance of providing strict definitions of privacy rights in line with the evolving understanding of human rights instruments.

***

In general, the R.Q. is a subset of the wider question as to 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 policy that enhances the protection of human rights. It builds on the academic literature that promotes the possibility, and necessity, of reconciling the two (chapters 2 and 3).

The R.Q. contains both an 'if' and a 'how' question, to which the various hypotheses refer. In relation to the 'if question', I submit that the trade-off model is not a useful intellectual device (I), that privacy rights are complementary with cybersecurity understood as NIS/narrow cybercrime (II), and that reconciliation can also be achieved in the case of broad cybercrimes (III). As to the 'how' question, which concerns the mode of reconciliation, I advance the following hypotheses: complementarity in the case of narrow cybercrime/NIS may be in the form of overlap (strong), causality (intermediate) or convergence (II a, b, c); reconciliation could mean that the measures necessary for an investigation are privacy agnostic (III a), which would be the case of narrow cybercrime/NIS, or, in the case of broad cybercrime, the trade-off could be avoided with the application of instruments featuring solid safeguards (III b). According to a final hypothesis (IV) relating to the 'how' question and tied to the reference to technology, hypotheses II-III cannot be fully demonstrated by means of classic legal analysis due to technology neutrality, the courts' apparent deference (to society) on technology, and the open-ended understanding of fundamental rights.

In terms of research methodology, answering hypothesis I requires performing descriptive and argumentative-theoretical steps, which are deductive in the case of the normative critique, and inductive for the methodological critique. Therein, I perform an analysis of terms (chiefly security, privacy and 'cyber'), which is heuristic and pragmatic, rather than etymological, and I adopt a law and society approach (developed with respect to 'privacy rights'). The selection of the case studies of deep packet inspection and LanGuardian was explicitly based on

proximity to the main argument; as for the relationship between the two cases, they can be viewed as falling within a most similar cases research design. Hypotheses II-IV require a mix of descriptive analysis and argumentative-empirical steps of a deductive nature. All research is desk research.

3 PLAN OF THE THESIS

In chapter 1 I illustrate the assumption that the trade-off model is normatively wrong, which I call the 'normative challenge', *vis-à-vis* Posner and Vermeule's trade-off model. The rejection of the trade-off model is premised on an understanding of the *ordre public* of the Union based on the rule of law and is directed at 'security v. liberty' in general. There, I appraise the relation between security and fundamental rights in the Union *vis-à-vis* its foundations, *ordre public* and the area of freedom, security and justice.

Chapter 2 concerns the first hypothesis, which I call the 'methodological challenge', and is premised on the inadequacy of the trade-off model due to (i) its misleading understanding of the terms of the equation, namely 'security' and 'privacy', (ii) its assumption that trading rights for security is the most efficient option, a questionable premise because (iii) the trade-off does not take into account all terms of the equation, particularly technology. I develop the methodological challenge with reference to security (in the context of terrorism) and privacy, understood as two interrelated but independent rights, namely respect for private and family life and the protection of personal data.

In chapter 3 I apply the normative and methodological challenge to map the field of cyber-security after Snowden's revelations, identifying its components, the EU applicable law, and ultimately reformulating the relationship between privacy rights and cybersecurity as embodied in offences or other legal provisions. It is by reasoning on such reformulations that it is possible to address questions of efficiency concerning trading-off 'security' with 'rights', and bring to the surface the role played by technology, so as to prove the over-simplification and intellectual emptiness of the trade-off model.

This is the objective of chapter 4, where the analysis demonstrates the validity/soundenss of the second assumption, corroborates hypotheses IIa and b on the complementarity between narrow cybercrime/NIS and privacy rights, and supports hypothesis IIa on the possibility of reconciling privacy rights with the fight against cybercrime. While the analysis proves the emptiness of the trade-off model, it does not automatically confirm the hypotheses, for which it is necessary to take into account technology. There, I use deep packet inspection as an example. The analysis introduces hypothesis IV, whereby classic legal analysis is viewed as insufficient to appraise the relationship between security and rights.

In chapter 5 I expound hypothesis IV, by explaining that classic legal analysis suffers from the consequence of technology neutrality and courts' avoidance to discuss matters of technology, as well as their open-ended understanding of rights. After reviewing existing attempts to appraise the impact of technology on rights, I devise a methodology that can link the legal and technological understandings of cybersecurity and privacy rights. To do so, I propose spelling out the technical and legal understanding of information security and privacy, and observe their interaction. In particular, I build on the notion of protection goals, attributes and cores.

Chapters 6 and 7 contain a re-appraisal of the right to respect for private and family life, and protection of personal data respectively, by identifying their attributes, i.e. the smallest elements of rights. On that basis I attempt to ascertain core areas of both rights, going beyond those identified by the CJEU. In addition, I describe a potential test for permissible limitations couched in article 52 of the Charter.

In chapter 8 I cross the technological understanding of privacy rights and information security based on protection goals, and then run a trial test of the methodology. Testing the method embodies the possibility that the responses to hypotheses (II) and (III) could be challenged, but also opens up avenues for new considerations of the 'how' questions that were originally buried under the weight of the trade-off model, namely the need for law and politics to re-appropriate issues of technology.

In the conclusions I sum up the findings and illustrate research and policy outcomes, as well as avenues for taking this research forward.

4 SCOPE

4.2 RELATIONSHIP WITH FUNDING PROJECTS

This thesis was co-financed by two FP7 projects, SurPRISE (Surveillance, Privacy and Security) and SURVEILLE (Surveillance: ethical issues, legal limitations and efficiency), and it is therefore important to clarify their import on my work.

The SurPRISE project challenged the trade-off model by taking into account citizens' perceptions, using surveillance-orientated security technologies as a concrete substantiation of 'security v. privacy'. The empirical phase built on a scholarly criticism of the trade-off model, which used technology as 'case studies' (chapter 1, section 2.5). It resulted in a series of recommendations and a decisions support system for consulting citizens on technological matters.

The SURVEILLE project developed a comprehensive method that took into account legal, ethical and technological considerations to discriminate between different surveillance technologies employed by end-users, and also paved the way to a decision support system for policy-makers.

This thesis builds on and develops substantially the work I carried out in both projects.

Part one of this thesis (chapters 1-4), which contains the theoretical critique to the trade-off model in general, and in particular with reference to cybersecurity, develops the research conducted within the SurPRISE project (and particularly Work Packages 3 and 5).

Part two of the thesis (chapters 5-8), which proposes a method to appraise the relationship between measures to tackle security issues and privacy rights that factors in the role of technology, is in dialogue with the SURVEILLE project (particularly Work Package 2).

Yet, the eight chapters of this thesis are based on fresh research and hence contain for the most part novel material (any references to the projects are properly noted in footnotes). In particular, the SurPRISE approach of taking technologies as a practical substantiation of case studies has been developed so as to take into account the context in which such technologies are used, in this case the cybersecurity policy as a complex case study. As for SURVEILLE, this thesis innovates in that it performs a direct attempt to bridge law and technology, i.e. to understand the direct impact technology has on the law, or the hidden link between law,

Human Rights and technology, instead of treating the two as separate fields dominated by different logics.

4.3 WHAT THIS THESIS IS NOT ABOUT

This thesis lies at the intersection of information technology law, Union law, fundamental rights law and technology assessment. It is concerned with the relationship between cybersecurity and privacy rights from the perspective of the latter as understood in Union law. Although it focuses on substantive criminal issues, it does not take a criminal law stance, and both procedural and jurisdictional issues are firmly outside the scope of this work.

Although one important conclusion will concern the regulation of technology, the thesis is not about regulatory models for technology, let alone how technology substitutes regulation; I will touch upon the matter in chapters 5 and 8. In this respect, while I am mindful of developments in the field of privacy by design, which I do occasionally mention (e.g. chapter 2, 5, 7 etc.), I do not take up the challenge of proposing how existing technologies could be improved by its application.

The general conclusions will reflect on tangential questions raised by this thesis that will be tackled by means of future research.

NB: case law and legislation referred to in the thesis date to August 2016.

PART 1 - MOVING BEYOND THE TRADE-OFF MODEL

CHAPTER 1 - TRADING SECURITY WITH LIBERTIES IS NORMATIVELY WRONG (NORMATIVE CRITIQUE)

We can no longer afford to take that which was
good in the past and simply call it our heritage,
to discard the bad and simply think of it as a dead
load which by itself time will bury in oblivion.
Hannah Arendt[61]

The purpose of this chapter is to expound the first assumption of this thesis (introduction, section 2), i.e., that 'security v. privacy' is a specification of the security versus rights model, which I argue is a fallacious, value-laden political choice "claiming the mantle of legality",[62] or rule *by* law[63] (as opposed to rule *of* law), and as such should be rejected in the EU, which is the jurisdiction of choice of this study.

In order to illustrate the 'normative critique', i.e. the idea that security v. liberty is normatively wrong, I refer to Posner and Vermeule's[64] trade-off model, which I describe in section 1. There, I lay the foundations for a normative and methodological criticism of the model with reference to the EU. To be sure, as a political and constitutional matter, the trade-off can be assessed in the light of the *ordre public* (public policy) of any polity. In this respect, my criticism of a theory originating in the US by no means translates into a criticism of US politics and policies,[65] nor into claims of a supposed normative superiority of the EU.

The normative challenge rests on four grounds, each addressed in a subsection. Thus, in section 2.1 I explore the relation of the trade-off model with a general theory of politics. In section 2.2. I assess the assumption that government choices are not dysfunctional. Section 2.3 anchors EU political action within the remit of the rule of law. In section 2.4 I address the relationship between emergency and normalization, and briefly address the so-called

[61] Hannah Arendt, *The Origins of Totalitarianism* (Harcourt 1968) p. ix. The quote stems from the introduction to the first edition of the book, in 1950.
[62] Dyzenhaus (2012), p. 451.
[63] Jenkins (2014).
[64] Eric Posner and Adrian Vermeule, *Terror in the balance. Security, liberty and the courts* (Oxford University Press 2007).
[65] Jeremy Waldron, *Torture, Terrore and Trade-offs. Philosophy for the White House* (Oxford University Press 2010).

deference thesis. Finally, an additional sub-section, 2.5, discusses empirical research into the attitudes of European citizens, that challenges their presumed acceptance of the trade-off model.

The methodological critique of the trade-off (first hypothesis, i.e. the emptiness of the trade-off model as an intellectual device,) will be the object of chapter 2.

1 THE TRADE-OFF MODEL PRESENTED BY POSNER AND VERMEULE

Posner and Vermeule's[66] version of the trade-off (a theory of decision-making during emergency) is a useful point of departure to appraise the model. To begin with, the authors argue that security and liberty are comparable items that can be represented as two perpendicular axes delimiting an area of policy choices, which represents different combinations of security and liberty. Taking into account real-life scarcity of resources, they argue that policy combinations cannot be infinite, but must encounter a frontier "where security cannot be increased without corresponding decreases in liberty, and viceversa."[67] Assuming that contemporary (US) governments are not "dysfunctional",[68] Posner and Vermeule argue that current policy combinations lie at this frontier (i.e. they are Pareto-optimal[69]), and hence that we have exhausted the options that can simultaneously enhance both security and liberty.

While their thesis does not "hold that security should be simply maximised",[70] at times of emergency the executive does and should reduce civil liberties, because "they interfere with effective response to the threat."[71] The ensuing choice concerning the ideal combination of security and privacy must be entrusted to the executive branch, as opposed to the judiciary or

[66] Posner and Vermeule (2007).
[67] Adrian Vermeule, 'Critiques of the Trade-off Thesis' in David Jenkins, Amanda Jacobsen and Anders Henrikens (eds), *The Long Decade. How 9/11 Changed the Law* (Oxford University Press 2014), p. 32.
[68] Posner and Vermeule (2007), p. 26.
[69] Gregory Mankiw, *Principles of Economics (7th edition)* (Cengage Learning 2013).
[70] Posner and Vermeule (2007), p. 37.
[71] Ibid, 4.

parliament. This is known as the 'deference thesis', and it hinges on the idea that courts and parliaments are governed by procedures which are too slow to cope with emergencies, as supported (in the authors' view) by historical evidence. The trade-off and deference theses are concerned with the institutional allocation of authority to evaluate policies taken at times of emergency (the second order question). Their target is the support advanced by civil libertarians for judicial review at times of emergency, as against the panicky and irrational policy-making of government. As for the first order question, *viz.* the cost and benefits of security policies, Posner and Vermeule refer to their lack of "expertise regarding the optimal security policy",[72] an anyway arduous enterprise due to the uniqueness of each emergency.

Vermeule contends that the many critiques which they have received, seemingly aimed at the trade-off thesis, actually target the deference thesis, leaving their trade-off model unchallenged.[73] While the doctrinal fight of legal philosophers continues,[74] I argue that both theses can be challenged on several grounds. To this effect, the trade-off thesis could be divided into two limbs: (i) 'civil liberties hinder an effective response to the threat'; and (ii) 'the executive should reduce civil liberties at times of emergency' (because we already find ourselves at the frontier). These limbs suffer from normative and methodological fallacies relating to two points that Posner and Vermeule gratuitously chose not to address: the cost-benefit analysis, and a general theory of politics.

I begin with the cost-benefit analysis. Posner and Vermeule clarify that they cannot indicate the optimal security policy, because they are unable to perform the necessary cost-benefit analysis. Yet, they make a number of crucial claims in the opposite direction. First and foremost, as cited above, "civil liberties interfere with an effective response to the threat". Second, they claim that measures taken after 9/11 are less drastic than those taken in the past. Third, they argue that policy-making during emergencies is of a similar quality to policy-making at normal times, so that, on average, measures taken are both accurate and effective, while courts (and parliaments) are, by contrast, less capable of delivering suitable responses to emergencies. Finally, while preventing abuses ensuing from security policies would be desirable, they must be factored in as a cost of emergency policy-making.

[72] Ibid, p. 6.
[73] Vermeule (2014).
[74] For an interesting summary of the different positions, see Patrick Herron, 'Beyond Balance: Targeted sanctions, security and republican freedom' in Elisa Orrù, Maria Grazia Porcedda and Sebastian Volkmann (eds), *Surveillance and control beyond the security v. privacy model* (Nomos Verlag forthcoming).

These claims, I would argue, raise three procedural challenges that will underpin the methodological critique (hypothesis I) I conduct in chapter 2. First, the authors take for granted the meaning of security and liberty, as if they were two monolithic concepts. Secondly, although the authors say they rely on heuristics, their claims presuppose some sort of measurement: 'effective', 'aggressive', 'accurate' responses can be judged only vis-à-vis a standard. One wonders if it is a 'Fox and the Grapes' issue, in that Posner and Vermeule claim that it would be hard for lawyers to assess emergency policies in all circumstances. This may be true of any specialist alone, but particularly so if only referring to the trade-off diagram. Indeed, using two axes may tell only part of the story, making it difficult to assess security-related policies. An important missing line of thought concerns technology, which has a practical bearing on what can and cannot be done.[75] Research attempting to measure emergency policies, by adding interdisciplinary depth (chapter 5, sessions 2 and 3) to the subject matter, are bearing interesting fruits.[76] Thirdly, those claims are by no means marginal: they are taken as a prerequisite of their whole argument. The trade-off thesis rests on an axiom which assumes that the average optimal security policy is followed, i.e. it is efficient. It is quite clear that, if we accept at face value (i.e., setting aside the normative implications) that the government will make, on average, the best choice humanly possible for a given society, the trade-off thesis cannot pose any problems. But what if the assumption does not hold? This opens a fatal wound in the thesis. Using Posner and Vermeule's words, it would take a dysfunctional government (and population) to overlook existing mechanisms of derogation from civil liberties, and to adopt instead ineffective, harshly aggressive measures paving to long-term abuse. In fact, such government would probably be identified with an undemocratic country operating against the rule of law.

This leads to the normative criticism. Whereas Posner and Vermeule eschew a "general theory of politics or judicial review",[77] their claim that we live in a world of scarce resources is a heavy political assumption, fitting well in a wider definition of politics. If anything, the usefulness of the trade-off model is that it reminds us that we *may* have to allocate scarce resources through political choices. Ultimately, all that matters in the trade-off is what concrete combination of security and liberty is chosen within a given policy (which is

[75] Jef Huysman, *The Politics of Insecurity* (Routledge 2006).
[76] Among others, the work of the SURVEILLE and SurPRISE projects.
[77] Posner and Vermeule (2007), p. 21.

different from saying that these are the only considerations in emergency policy-making) and polity. In sum, the choice of a suitable response to a security issue is deeply political.[78]

The deference thesis can be criticised on similar grounds. To begin with, the acceptability of the claim whereby the executive is best placed to intervene in the immediate aftermath of an emergency can only be appraised in relation to the form of government and legal tradition of a specific jurisdiction. Second, visions of insecurity – deriving from human (un)intentional action - are intertwined with the vision of politics advanced. Notably, the deference thesis does not contemplate appraising the duration of insecurity caused by an emergency. Much (in my opinion, well-founded) criticism has to do with the fact that what could be acceptable for a limited time – i.e. the executive taking over - becomes the norm.[79]

The normative and methodological claims, whereby civil liberties should be and are indeed reduced because they hamper security, must be discussed on similarly normative and methodological terrain. My interim conclusion is that the trade-off thesis is methodologically flawed regardless of the jurisdiction, because it unduly flattens and also reduces the variables to be taken into account. By contrast, the normative critique, i.e. appraising the extent to which it is desirable that a government surrenders constitutionally recognized rights, is context-specific. The two critiques share an important point of connection. The scope and understanding of some variables, in particular the meaning of security and liberty, will depend on the specific jurisdiction.

The impact of such a claim on comparability across jurisdictions, while relevant, is beyond the scope of this research and will not be further explored. In the same vein, although my critique may well be applicable to the US, I am not going to engage in an analysis of the American case. My analysis is strictly limited to the EU, which will be the framework for the normative and methodological critique I set out to develop in this and the next chapter. I begin by addressing the normative critique.

[78] Huysman (2006).
[79] Solove (2011); Jenkins (2014).

2 THE NORMATIVE CRITIQUE TO THE TRADE-OFF (AND DEFERENCE) THESES

I begin the analysis of the trade-off model in Europe by addressing the normative critique, which logically comes before the methodological critique because the terms security and liberty are normatively charged and determined. As a caveat, I must stress that mine is a normative argument: it concerns prescription, what ought to be, mindful of the interconnectedness between politics and *ordre public*. This is not to say that, within the EU, security has never been traded with liberties, nor that this will not happen.

The normative critique is articulated around the main claims made by Posner and Vermeule.[80] They maintain that (i) we live in a world of scarce resources (such as security and liberty). Since current policy combinations of security and liberty lie at the frontier, and (ii) our governments are not dysfunctional, we have exhausted the options that can simultaneously enhance both security and liberty, so that (iii) the executive should reduce civil liberties (iv) at times of emergency. Although Posner and Vermeule concede that it would be better if the government avoided abusive behaviours, they do admit that arbitrariness may be justified. Such claims are based on heuristics and do not engage with a general theory of politics or judicial review (v).

My first point of criticism is that addressing the trade-off between scarce resources (i) belongs intrinsically in and must be addressed as part of a general theory of politics (v) (and judicial review). As a starting point to unveil the fallacies of a simplistic trade-off model, I therefore carve a working definition of politics (section 2.1). The second point of criticism is that the idea that governments are not dysfunctional (ii) is a heavy assumption at odds with the *ordre public* of the Union, which was built against the tragic experience of dysfunctional governments that led to the catastrophe of WWII (section 2.2). The third point is that such background informed the constitutional architecture of the Union, which features constraints against reducing civil liberties, also in the AFSJ (section 2.3). The fourth point consists in a review of the most insidious claim, that concerning emergencies (v), which calls for a reflection on norms enshrined in the Lisbon Treaty and examples of cases that could be seen as stress-testing the *ordre public* (section 2.4); there, I briefly discuss the question of

[80] Posner and Vermeule (2007).

normalization. Lastly, I touch upon the ostensible desire of citizens to exchange liberty for security (section 2.5).

2.1 TRADING SCARCE RESOURCES IS ABOUT A GENERAL THEORY OF POLITICS

Here I address the first critique of the trade-off model, whereby trading-off security and liberty as conflicting scarce resources (i) is a choice of a political nature (v), whose appraisal warrants a digression on the meaning of politics and law. Politics has, in fact, been described as an ontologically composite concept aimed at solving controversies over scarce resources:

> *"A complex process hinging on a progression of intertwined events and actions, whereby, within any organized community, a multiplicity of actors reaches binding collective decisions aimed at settling controversies coming up within the community or in its external relations."*[81]

According to this definition, besides the prerequisite (conflict over scarce resources), politics is made up of three additional elements: the scope (the organized community), the aim (resolution of conflict) and the means towards the aim (binding collective decisions).[82]

Clearly the scope of this discussion is the EU, which is a *sui generis*,[83] open-ended community made of several organized communities, its institutions and Member States – the latter playing a much more prominent role than usually portrayed by integration scholars[84]– and organized chiefly in accordance with its 'constitution',[85] the Treaty of Lisbon. A digression on the abstract concepts that form the definition of politics is instrumental to this part of the normative critique.

---

[81] Virgilio Mura, *Categorie della Politica. Elementi per una teoria generale* (Giappichelli Editore 2004) 115. "Un processo complesso, imperniato su successioni concatenate di eventi ed azioni, attraverso il quale, nell'ambito di una qualsiasi convivenza organizzata, una pluralità di attori perviene a prendere le decisioni collettive vincolanti finalizzate a dirimere I conflitti che insorgono nel proprio interno e/o nei rapporti esterni." Translation mine.
[82] Ibid.
[83] Opinion of the Court of 18 December 2014, Avis 2/13, EU:C:2014:2454, paras 157 and 158.
[84] Alan Milward, *European Rescue of the Nation State* (Taylor and Francis 1999).
[85] The Treaty was first seen as the basic constitutional charter of the then Community in Judgment of 23 April 1986 in Les Verts v. Parliament, C-294/83, EU:C:1986:166, para 23. Although the judgment referred to the European Community Treaty, I follow Cremona's argument that the Treaty on the European Union and the Treaty on the Functioning of European Union must be read as legally interwoven texts. Marise Cremona, 'The Two (or Three) Treaty Solution: The New Treaty Structure of the EU' in Andrea Biondi, Piet Eeckhout and Stephanie Ripley (ed), *European Union Law After the Treaty of Lisbon* (Oxford University Press 2012).

One fundamental concept underlying Posner and Vermeule's first and second claims is scarce resources. What are scarce resources, and how does this apply to security and liberty? Scarce resources are usually understood as assets that are or can be made excludable, rivalrous, or both,[86] paving the way to conflict; such conflict is first of all of a material or physical nature. A classic example of excludable and rivalrous resources is that of commodities, land, and water. The comparison with commodities, however, does not seem to easily adjust to security and liberty. Let us then take the elements that engender scarcity. It seems safe to claim that liberty and security are *understood* as being for all, so that they are not excludable.[87] Rather, the claim in the trade-off is that they are rivalrous, and hence scarce, thus triggering a controversy. It is by expounding this controversy within a wider theory of politics that some light can be shed. Such controversy is more of an immaterial or theoretical nature. The kind of assets making security and liberty rivalrous, paving the way to antinomies,[88] but not excludable, are values. And it is precisely the controversy caused by the plurality of values, which, according to Weber, is quintessential to politics.[89]

Values as assets carry a double valence. On the one hand, they are axioms containing worth *per se*, all meriting equal respect; in this sense, values exist before and beyond the law (though sometimes the two notions coincide, such as in the German doctrine of *Drittwirkung*[90]). On the other hand, values can be encapsulated in rules of behaviour and bear prescriptive content, such that they become principles;[91] in this sense, they can acquire legal force as foundational principles, general principles or policy-oriented principles.[92] The specific subset of values chosen by a community (as a result of any controversy), and the related principles, contribute to the formation of the community's (political) identity and constitute its (legal) ideal **ordre public,** understood as public policy[93] or constitutional

[86] On goods, see Mankiw (2013).
[87] Though they can be made excludable, becoming prerogatives. On goods, see also Waldron (2010), chapter 5.
[88] Norberto Bobbio, *L'Età dei Diritti* (Einaudi 1997).
[89] Max Weber, *La Scienza come Professione. La Politica come Professione* (Einaudi 2004).
[90] Francesca Angelini, *Ordine pubblico e integrazione costituzionale europea. I princìpi fondamentali nelle relazioni interordinamentali* (Cedam 2007).
[91] Ibid; Marise Cremona, 'Values in EU Foreign Policy' in Panos Koutrakos and Malcolm Evans (eds), *Beyond the Established Orders Policy Interconnections between the EU and the Rest of the World* (Hart Publishing 2011).
[92] Angelini (2007). On principles and values in different disciplines, see Armin von Bogdandy, 'Founding Principles of EU Law: A Theoretical and Doctrinal Sketch' (2010) 16 European Law Journal.
[93] Corresponding to ordèn publico, offentliche ordnung, ordine pubblico.

architecture[94] (also the boundary preserving a jurisdiction's legal integrity vis-à-vis external intereferences[95]), as against **law and order** or **material ordre public**, that is, policing.[96]

Both foundational, general and policy-oriented principles inform the choice of means of resolution of a controversy, informing in turn binding collective decisions. These are decisions that affect the community as a whole, regardless of how many actors ('a multiplicity') contribute to the adoption of decisions, and of the procedures followed ('the progression of intertwined events and actions'). Arguably, a decision is binding if, in principle, it can be imposed upon the recipients to the extent that the controversy is appeased; a successful resolution of the controversy paves the way to its legitimacy. Decisions can be imposed on the community through economic, ideological, normative and coercive power. Coercive power consists in either the threat of physical force, or its actual use, regardless of the procedures and individuals exerting violence. It contemplates both a Hobbesian scenario of the state as the only antidote against the condition of *homo homini lupus*, as well as Weber's view,[97] acknowledged in article 2.4 and 51 of the Charter of the United Nations and article 4 TEU, that the post-Westphalian State[98] is the monopolist of the legitimate use of physical force, which however serves other purposes.[99] In both circumstances, it represents the measure of last resort to impose the settlement of a controversy over a community, so as to maintain "the territorial integrity of the State…law and order and…national security" (article 4 TEU). The extent to which a community relies on coercive power is a function of its *ordre public.*

Whichever the methods chosen, the aim is resolving minor or major controversies, so as to **secure** the continuity of a given community. In legal terms, the resolution of controversies can take the form of the restoration of law and order, welfare-related decisions, laws, sentences, peace, and ultimately entails the reaffirmation of sovereignty[100] and of a particular *ordre public* understood in terms of the jurisdictional identity of a community/constitutional architecture. In fact, different communities face different controversies, and the means (principles) chosen by a given community to solve a specific controversy reflect back on the

[94] Angelini (2007).
[95] Ibid.
[96] Ibid.
[97] Weber (2004).
[98] Antonio Cassese, *International Law (2nd edition)* (Oxford University Press 2005).
[99] Huysman (2006) rejects the trade-off model because the enjoyment of liberties is predicated on security.
[100] In the sense of control over a territory, population and jurisdiction. Cassese (2005).

organizational principles of that community, and subsequent controversies, in a continuous circle.

The constitutional architecture feeds into and is nurtured by specific ways of addressing controversies. Such reaffirmation is strongly linked to the abstraction of what **the good life** means within a given community;[101] that is, the ideal of life or *vouloir-vivre* to which members of a given community aspire.[102] In this respect, security can serve the interest of *vouloir vivre* either understood as Hobbesian survival, or as a communal life devoted to certain goals (e.g. the enjoyment of rights). The *Bundesverfassungsgericht* judgment on the ratification of the Lisbon Treaty[103] can be read as offering a glimpse into what matters for *the vouloir vivre* of a particular nation, which unsurprisingly includes determining the scope of criminal liability,[104] i.e. of goods and wrongs.

In conclusion, Posner and Vermeule bring to the surface only the outcome of a controversy – security v. liberties – without looking into its nature and the alternative means of settling that controversy, so that 'security v. liberties' tautologically justifies itself. Posner and Vermeule's reliance on heuristics is an elegant avoidance of the crux of the matter: namely, to what extent trading liberty with security is consistent with a community's constitutional architecture, and the implications of such a choice for the community's *ordre public* and ideal of the good life, which demand a discussion of theories of politics (and judicial review). It is on this ground that a normative appraisal of the trade-off theory becomes possible. I can now move to the second element of criticism of the trade-off model.

[101] Hannah Arendt, *The Human Condition (2nd edition)* (The University of Chicago Press 1998); Charles Taylor, *Sources of the Self. The Making of the Modern Identity* (Cambridge University Press 1989).
[102] Abdelkhaleq Berramdane, 'L'Ordre Public et les Droits Fondamentaux en Droit Communautaire et de l'Union Européenne' in Various authors (ed), *Territoires et liberté Mélanges en hommage au Doyen Yves Madiot* (Bruylant 2000). Quoted in Angelini (2007). Quoting Bernardone (p. 217).
[103] The judgment has been seen as expressing unmerited criticism, as a *cri de coeur*, due to the cumulation of resentment toward certain institutional arrangements. Jean-Claude Piris, *The Lisbon Treaty. A Legal and Political Analysis* (Cambridge 2010).
[104] "Particularly sensitive for the ability of a constitutional state to democratically shape itself are decisions on substantive and formal criminal law (1), on the disposition of the monopoly on the use of force by the police within the state and by the military towards the exterior (2), … decisions on the shaping of living conditions in a social state (4) and decisions of particular cultural importance, for example on family law, the school and education system and on dealing with religious communities (5)." BVerfG, 2 BvE 2/08 Rn (1-421), Judgment of 30 June 2009, para 252, determined in paras 253 to 260.

2.2 'GOVERNMENT IS NOT DYSFUNCTIONAL' IS A BIASED ASSUMPTION, OPPOSED TO THE FOUNDATIONS OF THE UNION *ORDRE PUBLIC*

The lesson to be taken forward is that communities are constantly shaped by the nature of the controversies which they face; in this respect, the current history of the European Union is (sadly) a thriving field of experimentation. Some controversies are obviously more relevant than others, and sometimes reveal their strength only with hindsight.[105] It is one such controversy that challenges the blind reliance on the executive, and allows me to elaborate my second critique to Vermeule and Posner's trade-off thesis. The moral and political foundations of post WWII Europe,[106] and the later Union, hinged on 'anti-fascist' (as a shorthand for anti-authoritarianism and anti-totalitarianism[107]) values, to the effect that no government is worthy of automatic trust, and must be embedded in a web of checks and balances, particularly *vis-à-vis* fundamental rights.

Before addressing these constraints, I wish to substantiate the claim that such values laid the foundations of the Union. While I can eschew the history and theories of European Union integration, which has been extensively covered by a rich literature,[108] for the sake of an honest discussion, it must be recalled that the adoption of 'anti-fascist' values was delayed by the interaction (and ensuing controversies) between the WWII victors and the Member States.[109] Notably, the Coal and Steel Community stayed clear of the values expressed by

[105] E.g. Weiler's reflections on Europe after Brexit: Joseph HH Weiler, '¿Qué te Ha Pasado, Europa?' *El País* (Madrid), 8 July 2016.

[106] Federico Romero, 'Antifascismo e Ordine Internazionale' in Alberto De Bernardi and Paolo Ferrari (eds), *Antifascismo e Identità Europea* (Carocci 2004).

[107] The expression used here refers to the historical coalition of forces that fought Nazism and Italian Fascism. In political science some understand Italian Fascism as a borderline authoritarian, rather than a totalitarian, regime (limited pluralism and reduced mobilization v. no pluralism and high mobilization). Maurizio Cotta, Donatella Della Porta and Leonardo Morlino, *Scienza Politica* (Il Mulino 2001); Arendt (1968), *The Origins of Totalitarianism*. Arendt saw and highlighted the difference, especially in terms of mobilization. However, the two forms of government share the characteristics of impaired pluralism, exclusion of citizens from decision-making and the unfettered power of the governing leader or coalition, which is what makes the distinctions irrelevant for the legal discussion underway. More important is the historical distinction between anti-fascism and anti-totalitarianism. Since the coalition against Fascism included a strong Communist component, anti-fascism did not originally entail anti-totalitarianism. A thorough discussion can be found, in Italian, in Alberto De Bernardi and Paolo Ferrari (eds), *Antifascismo e Identità Europea* (Carocci 2004).

[108] André Fontaine, *La Tache Rouge. Le Roman de la Guerre Froide* (Editions de la Martinière 2004); Leonardo Rapone, *Storia dell'Integrazione Europea* (Carocci 2004); Milward (1999). On theories of integration, see ibid; Paul Craig and Gráinne de Búrca, *European Union Law: Text, Cases and Materials* (Oxford University Press ed, 2015).

[109] For the WWII victors, the most urgent controversy was not fascism, but rather halting the expansion of the Soviet Union: Romero (2004). To prevent the 'old continent' from slipping again into war without falling prey to the Soviet bloc, the United States invested in 'freeing' European member states 'from want' (see chapter 2, section 2.1) through the Marshall Plan (ibid; Rapone (2004).). Then, they founded NATO, and occasionally strengthened remnant national fascist forces to counter-balance local communist parties (with the exception of

European anti-fascist movements – democracy, the rule of law and respect for human rights – and focussed instead on the allocation of two scarce (excludable and rivalrous) commodities, coal and steel, which had been at the source of the use of physical force in both World Wars.[110] Angelini rightly described the Union's first approach as an economic *ordre public*.[111] Similarly, the creation of a defence and political community was soon defeated as too diplomatically audacious a project. Yet, 'anti-fascist' values acted as the moral and political roots of post-War Europe.[112] They informed several European post-WWII Constitutions[113] – leading from the *état legal* to *état de droit*[114]– and the Convention founding the Council of Europe,[115] as illustrated in its preamble. Following from the discussion in section 2.1, the shift was both in values and in organizational principles, including the means to settle controversies.

On the one hand, the aggressive policies of Nazism and Fascism were notably accompanied by an organicistic ideology (sets of values) of society,[116] coercing individuals into conformism, and unfetteredly expelling (or worse) the non-conformist from within to ensure the survival of the coherent group. The disregard of the individual, who is at the heart of modern conceptions of democracy as an autonomous citizen endowed with rights[117] and capable of spontaneous action,[118] entailed "the absolute denial of fundamental rights".[119] For Cassin WWII was "the 'human rights war' inflicted on people by those who espoused a monstrous racist doctrine, and waged simultaneously against man and the community of men, with unprecedented systematic cruelty".[120]

Germany). Another obstacle to the outright embracing of anti-fascist values within the integration process was the colonialist legacy of various founding Member States (Romero (2004); Fontaine (2004).) Indeed, early steps toward integration concerned only what was diplomatically feasible among countries.

[110] Rapone (2004).

[111] Angelini (2007).

[112] Romero (2004).

[113] Stefano Ceccanti, 'L'antifascismo e le Nuove Costituzioni Democratiche' in Alberto De Bernardi and Paolo Ferrari (eds), *Antifascismo e Identità Europea* (Carocci 2004).

[114] As the Kelsenian constitutionality check of the acts of the legislature *vis-à-vis* constitutional principles, notably human rights. Charles Leben, 'Is there a EU Approach to Human Rights?' in Philip Alston, Mara Bustelo and James Heenan (eds), *The EU and Human Rights* (Oxford University Press 1999).

[115] Jonas Christoffersen and Mikael Rask Madsen (eds), *The European Court of Human Rights between Law and Politics* (Oxford University Press 2011).

[116] Organicistic societies tend to preserve the collectivity over the individual, and are typical of primitive legal orders. Bobbio (1997).

[117] Ibid.

[118] Hannah Arendt, 'Freedom and Politics: a lecture' (1960) 14 Chicago Review 28-46; Arendt (1998), *The Human Condition*.

[119] Leben (1999), p. 87.

[120] Quoted in ibid.

On the other hand, the resort to coercive means to impose the settlement of a controversy over a community was a hallmark of such repressive regimes, and was expressed in the conflation of **the material and ideal notions of ordre public**. The maintenance of law and order was superimposed onto public policy, as resulting from autocratric decisions resting on ideologies of homogeneity[121] aimed at stifling spontaneous action and, thus, difformity.[122] The integrity of the state was identified with the maintenance of the ideological organization of a homogenous, organicistic society, maintained through a range of means, from indoctrination, throught socialization (mobilization and regimentation), to the arbitrary application of power and violence by state institutions, to terror.[123] In conclusion, such regimes were characterized by the permanent conflation of the two notions of *ordre public*, where broad police powers would be constantly expanded for the sake of reaffirming the objectives of the regime (its executive-leader), at the expense of both the exercise and guarantees of civil liberties.[124]

As a repudiation of such experiences, the individual regained the central place acquired through modernity, thanks to the myth, or fiction, of inalienable rights justified by the inherent dignity of the human being.[125] The means to reach binding decisions to resolve any kind of controversies were to be reidentified in democratic processes, a solid application of the rule of law to prevent the abuse of power, and the progressive respect of an increasing range of fundamental rights. The three are inextricably linked, in that only individuals fully enjoying their rights and freedoms can be autonomous citizens taking part in the administration of the state, and the preservation of rights and freedoms comes from the application of restrained power, shared as widely as possible.[126] Democracy and human rights are mutually reinforcing objectives, whereby the rule of law is both the means to achieve them, and their procedural substantiation.

Such a move recognizes both the need that individual freedom must be regulated for the sake of a peaceful human society and that there are times when extreme measures may be taken, but with fundamental qualifications.

---

[121] Donatella Della Porta and Herbert Reiter, *Polizia e Protesta. L'Ordine Pubblico dalla Liberazione ai "no global"* (Il Mulino 2003). See also literature in Angelini (2007).
[122] Arendt (1960), 'Freedom and Politics'.
[123] Ibid.
[124] See the literature concerning Italian Fascism in Angelini (2007).
[125] Bobbio (1997); Antonio Cassese, *I diritti umani oggi* (Laterza 2012).
[126] Bobbio (1997).

On the one hand, the exercise of most rights (so-called qualified rights) can be restricted vis-à-vis pressing social needs, such as ensuring public security, law and order, public health, the life and freedom of others or even, at the extreme, facing war. Yet, even if in a restricted form in the face of pressing social needs, rights must always be guaranteed,[127] which underpins the idea of the 'essence' of rights in article 52 of the Charter of Fundamental Rights of the European Union[128] (hereafter the Charter). In other words, rights can never be interfered with to the point that they cease to exist. Another important point has been the recognition, perhaps rooted in religious tradition, that even those who endanger democracy and rights deserve to be treated humanely and have their rights respected, against the calls of an "enemy criminal law".[129]

On the other hand, during an emergency, maintenance of law and order can be crucial to preserve the existence of a community. All elements feed into each other to create both law and order, and *ordre public* in the ideal or normative sense (public policy): through both the protection of the most important values (and thus the allocation of tangible and intangible resources) from the outside, and reaffirmation inside. To this effect, the possibility of applying limitations and exceptions is granted, provided a number of caveats are respected.[130] When, however, the state of emergency becomes permanent, and emergency measures based on the pre-eminence of law and order become the norm, i.e. they are normalized, they reflect a policy approach akin to repressive regimes, such as fascism. Accordingly, the ideal notion of *ordre public* cannot be conflated with the material notion, which would lead to the paradox of limiting constitutionally guaranteed freedoms, beyond what the foundational text has envisaged, in the name of the constitutional order.[131]

The shift to human rights was neither smooth nor immediate, as highlighted above, as the requirements of the fight against international communism led to a resort to realpolitik and in

[127] E.g. in relation to the first sentence of the Italian Constitutional Court, Angelini (2007).
[128] David Anderson and Cian C Murphy, 'The Charter of Fundamental Rights' in Andrea Biondi, Piet Eeckhout and Stefanie Ripley (eds), *EU Law After Lisbon* (Oxford Scholarship Online 2012); European Union Network of Independent Experts on Fundamental Rights, *Commentary of the Charter of Fundamental Rights of the European Union* (2006).
[129] Cassese (2012), *I diritti umani oggi*. Gunter Jacobs' *Feindstrafrecht* or 'enemy criminal law' is based on the idea that citizens who expressly choose to challenge the legal system become enemies, and do not qualify to enjoy the constitutional protections guaranteed to the law-abiding citizens, but rather deserve exceptional treatment. Stefan Braum, 'Are We Heading Towards a European form of 'Enemy Criminal Law'? On the Compatibility of Jakobs' Conception of 'an Enemy Criminal Law' and European Criminal Law' in Francesca Galli and Anne Weyembergh (eds), *EU counter-terrorism offences. What impact on national legislation and case law?* (Editions de l'Université de Bruxelles 2012).
[130] Council of Europe, Division de la Recherche de la Cour Européenne des Droits de l'Homme, *Sécurité Nationale et Jurisprudence de la Cour Européenne des Droits de l'Homme* (Council of Europe, 2013).
[131] Angelini (2007).

particular to fascist/authoritarian methods, notably curtailing pluralism, thus democracy, and an unrestrained use of violence to re-establish order. It would take multiple intertwined controversies for the *ordre public* of the Union to fully encompass its anti-fascist cultural and political roots,[132] of which it is worth recalling some, without pretence of exhaustiveness.[133] First, the reaction of German and Italian constitutional courts to decisions of the Court of Justice of the European Union (hearafter CJEU) favouring the Community's economic *ordre public* at the expense of human rights constitutionally protected by Member States.[134] Second, the demise of European colonialism leading Member States to submit to the authority of the ECtHR,[135] and the subsequent reaction by the CJEU to threats that the European Communities could accede to the ECHR.[136] Starting with *Internationale Handelsgesellschaft*,[137] the Court slowly built the system of safeguards of fundamental rights as we know it today (eventually earning its fame as champion of rights in the Union):[138] the primacy and autonomy of EU law; the hierarchy of sources, whereby rights form an integral part of the general principles of EU law, constitutional traditions are taken into account as a source of inspiration, and international treaties supply guidelines; and horizontal provisions regulating permissible limitations to fundamental rights.[139] Third, the fall of the Soviet Union and the end of the Cold War that paved the way to a wider reflection on democracy, the respect for fundamental rights and the rejection of authoritarian values at Member State and EU level,[140] which found a first complete expression in article 6(2) of the Treaty of Maastricht (moving from the economic to the political *ordre public*).[141] Fourth, the expansion of areas of Union competence with the Lisbon Treaty. Finally, technological evolution, which

[132] Romero (2004); De Bernardi and Ferrari (2004).
[133] Philip Alston, Mara Bustelo and James Heenan (eds), *The EU and Human Rights* (Oxford University Press 1999); Craig and de Búrca (2015); Stefano Rodotà, *Il diritto di avere diritti* (Editori Laterza 2012).
[134] As exemplified by the Solange I, Maastrich I and Arrest Warrant decisions, and Italian Constitutional Court decisions n. 98 of 27 December 1965 and n. 183 of 27 December 1973. Angelini (2007); Piris (2010).
[135] Christoffersen and Madsen (2011).
[136] An argument, based on new archival research, advanced by Bill Davies, 'Bottom Up or Top Down - The History of Human Rights in European Law (speech)' (Setting an Agenda for Historical Research in European Law - Actors, Institutions, Policies and Member States, Florence, European University Institute, 11 December 2015).
[137] Judgment of 17 December 1970 in Internationale Handelsgeselleschaft mbH v. Einfuhr- und Vorratsstelle für Getreide und Futtermittel, C-11/70, EU:C:1970:114.
[138] On judicial activism see Michal Bobek, 'Of Feasibility and Silent Elephants. The Legitimacy of the Court of Justice through the eyes of National Courts' in Maurice Adams and others (eds), *Judging Europe's Judges. The legitimacy of the case law of the European Court of Justice* (Hart Publishing 2013); Takis Tridimas, 'Primacy, Fundamental Rights and the Search for Legitimacy' in Miguel Poiares Maduro and Loïc Azoulai (eds), *The Past and Future of EU Law. The Classics of EU Law Revisited on the 50th Anniversary of the Rome Treaty* (Hart Publishing 2010); José Narciso Cunha Rodrigues, 'The Incorporation of Fundamental Rights in the Community Legal Order' in Ibid; Alston, Bustelo and Heenan (1999).
[139] Cunha Rodrigues (2010).
[140] Bobbio (1997).
[141] Angelini (2007); Piris (2010); von Bogdandy (2010).

brought about new needs and, correspondingly, new controversies ending with the acknowledgment of additional rights (chapter 2).

Such values were eventually embraced and refined through judicial interpretation, and today constitute the hard core of the EU *ordre public*,[142] to the effect that Piris has stated that the Lisbon Treaty is "deeply rooted in fundamental rights".[143] This lays the basis for the third critique to the trade-off model, which I illustrate below.

2.3 EU POLITICAL CHOICES ARE CONSTRAINED BY ITS *ORDRE PUBLIC* BASED ON THE RULE OF LAW

Thus far I set out to demonstrate that reducing liberties for the sake of security equates to conflating the material and ideal *ordre public*, which fits within an illiberal theory of politics, namely the 'fascist' one, the legacy of which led the Member States of the Union to build an *ordre public* (their own first, and that of the Union later) that would progressively constrain the executive, challenging any reliance on its 'functionality'. In this section I explore 'anti-fascist' values in greater depth, and describe the constraints that mould the political choices of the Union to the effect of hindering the option of 'reducing civil liberties' - my third challenge to the trade-off thesis.

The values and principles forming the EU *ordre public* are reaffirmed in the preamble,[144] as well as the body, of the Treaty on European Union,[145] notably article 2[146] on Common Provisions:

---

[142] A summary of which could be found in *Opinion of the Court 2/13*, paras 55-177.
[143] Piris (2010), p. 71.
[144] The rule of law is mentioned in two recitals, which read "Drawing inspiration from the cultural, religious and humanist inheritance of Europe, from which have developed the universal values of the inviolable and inalienable rights of the human person, freedom, democracy, equality and the *rule of law*" and "Confirming their attachment to the principles of liberty, democracy and respect for human rights and fundamental freedoms and of the *rule of law*" (emphasis added).
[145] Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU), OJ C 83/01 (Lisbon Treaty).
[146] Former article 6 TEU was different in that it read that the foundation of the Union consisted in 'principles', which only partly overlap with the values listed in article 2: "liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law." Some commentators saw the new wording as a retrenchment (among others, Damian Chalmers, 'Looking back at ERT and its contribution to an EU fundamental rights agenda' in Poiares Maduro and Azoulai (eds), *The Past and Future of EU Law* (Hart Publishing 2010)). With reference to the different uses of values and principles in the TEU, Cremona notes that the emphasis on values in article 2 refers to identity-building aspects, whereas reference to principles, as found for instance in article 21

> *"The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail."*

Article 2 is not simply a symbolic and political declaration. It is constitutional[147] or "super primary law",[148] forming the ideological basis for the policy objectives listed in article 3 TEU, and it also produces concrete legal effects.[149] A serious and persistent breach of the values listed in article 2 TEU by one Member State can trigger the application of the sanctions contained in article 7 TEU, as a (politico-legal) measure of last resort available if the mechanism of early warning recently devised by the European Commission fails.[150] Likewise, adherence to the rule of law is an essential precondition to enable a state to apply for membership of the Union as provided for by article 49 TEU. Furthermore, its content is a high priority of the EU, figuring second among the objectives of the EU,[151] arguably through the policies further mentioned in article 3 TUE (see *infra* section 2.3.2).

The founding elements of the EU *ordre public* listed in article 2 must be read together, as each requires the others in order to be substantiated. Yet, for the sake of conciseness, I look at them from the perspective of the rule of law as, to the extent possible, a fictitiously independent value-principle binding them all together. After the first legally binding reference

---

(CFSP) underscores the dimension of policies and actions. Cremona (2011). On the reciprocal value of article 2 and 21 see Ester Herlin-Karnell, 'EU Values and the Shaping of the International Legal Context' in Fabian Amtenbrink and Dimitri Kochenov (eds), *European Union's Shaping of the International Legal Order* (Cambridge University Press 2013). Angelini has noted that values acquire legal force only when contained in general principles or policy-oriented principles (Angelini (2007)). Moreover, if one takes an *Alexian* stance, if values must be respected, it means that the principles enshrined in secondary law must be consistent with such values and follow suit; see Robert Alexy, 'Constitutional Rights and Legal Systems' in Joakim Nergelius (ed), *Constitutionalism - New Challenges: European Law from a Nordic Perspective* (Brill 2008). Von Bogandy concisely but convincingly shows the open-ended meaning of principles in the EU (von Bogdandy (2010)). Accordingly, I disagree with those commentators for whom article 2 constitutes a rentrenchment. Mindful of the discussion in section 2.1, the reference to values in the founding text is consistent with a later clarification of principles, in accordance with such values, both by the legislature and the judiciary, which would have no lesser force as an interpretation of the constitutional Charter. Furthermore, the expression 'respect for human dignity and rights' could not be seen as excluding the Institutions' duty to take positive action toward rights, i.e. to protect and fulfil them, as stated in case law.

[147] von Bogdandy (2010).

[148] Allan Rosas and Lorna Armati, *EU Constitutional Law - An Introduction* (Hart Publishing 2010), p. 43.

[149] Piris (2010); von Bogdandy (2010).

[150] European Commission, *A New EU Framework to Strengthen the Rule of Law* ((Communication) COM (2014) 158 final, 2014). Poland came close to testing the article 7 procedure. Duncan Robinson and Henry Foy, 'Poland Faces Brussels' Ire over Media Reforms' *Financial Times* (London, 14 January 2016).

[151] Piris (2010).

made in *Les Verts,*[152] the value-principle[153] of the rule of law has gradually[154] acquired constitutional weight and the character of "dominant organizational paradigm".[155] Besides being one of the values relevant for the procedures laid down by articles 7 and 49,[156] the rule of law is a guiding principle of the Union's External Action,[157] it informs the functioning of the CJEU[158] and is referred to in article 14 of Protocol n. 4 on the Statute of the European System of Central Banks and of the European Central Bank. Furthermore, the rule of law features in the preamble of the Charter as one of the principles upon which the Union is founded (an expected reference, given the purpose of the rule of law being to enable the respect of human rights, through the implementation of democracy, as discussed *supra* and *infra*). The CJEU confirmed its nature of 'umbrella'[159] bearing interpretive value[160] and encompassing sub-principles actionable before a court, the general principles of EU law.[161]

[152] "It must first be emphasized in this regards that the European Economic Community is a Community based on the rule of law, inasmuch as neither its Member States nor its institutions can avoid a review of the question whether the measures adopted by them are in conformity with the basic constitutional charter, the Treaty". *C-294/83 - Les Verts v. Parliament*, para 23.

[153] Following Pech, referring to the rule of law as 'principle' or 'value' is interchangeable and does not entail any variation in the enforceability of the actions taken pursuant to it. Laurent Pech, *Rule of law as a Guiding Principle of the European Union's External Action* (CLEER Working Papers, Centre for the Law of EU External Relations, TMC Asser Instituut Inter-university Research Centre, 2013).

[154] It has acquired greater importance after the establishment of mutual recognition of judicial decisions. European Commission (2014), *COM (2014) 158 final*. It "seems to be developing along the lines of what can be called the substantive-ideal-type rule of law aligned with norms of substantive justice (in particular the right to a legal remedy)". Deirdre Curtin, *Executive Power in the European Union* (Oxford University Press 2009) chapter 7, p. 199.

[155] Laurent Pech, *The Rule of Law as a Constitutional Principle of the European Union* (Jean Monnet Working Paper Series, New York University School of Law, 2009), p. 50.

[156] According to Pech, articles 7 and 49 TEU turn the rule of law into a form of conditionality, a benchmark to evaluate the deeds of member states and the quality of potential applicants, an understanding unique to the Union and consistent with its legal status of supranational organization with conferred powers. Ibid.

[157] Article 21 TEU lists the rule of law as a principle that must guide the 'Union's action on the international scene' and which 'it seeks to advance in the wider world' by means of common policies and actions, and a high degree of cooperation in all fields of international relations. Pech (2013), *Rule of Law as a Guiding Principle of the EU's EA*.

[158] Pursuant to article 263 TFEU, the CJEU has jurisdiction "in actions brought by a Member State, the European Parliament, the Council or the Commission on grounds of lack of competence, infringement of an essential procedural requirement, infringement of the Treaties or of any *rule of law* relating to their application, or misuse of powers" (emphasis added).

[159] For a review of cases on the rule of law see Pech (2009), *The Rule of Law as a Constitutional Principle of the European Union*, Annex.

[160] Ibid.

[161] Takis Tridimas, *The General Principles of EU Law* (Oxford University Press 2006).

2.3.1 *THE TENETS OF THE RULE OF LAW AS ORDRE PUBLIC AND AS EMERGENCY BRAKE*

The tenets of the rule of law are both the defining elements of the *ordre public* and the emergency break constraining government's ability to trade-off liberty with security, irrespective of an emergency. The rule of law has "progressively become a dominant organisational model of modern constitutional law and international organisations"[162] (at least in its thin understanding), yet its tenets are open-ended, acquiring meaning only with practice. Indeed, due to its wide endorsement, there exist multiple definitions that reflect the objectives of the institutions that adopt it.[163]

I follow the list of tenets contained in the European Commission's Communication on the rule of law,[164] which reflects the post-WWII constitutional traditions of the Member States,[165] and widely corresponds to the tenets developed by the Council of Europe's Venice Commission[166] taking into account the ECtHR case law.[167] This is unsurprising, as the Council of Europe is seen as the general "benchmark for human rights, the rule of law and democracy in Europe."[168] Incidentally, it is in this respect that I follow Angelini's idea of a composite European *ordre public* reflected in article 6 TEU.[169] As a result, when I refer to the substance of each principle I take into account the interpretation of both the CJEU and the Council of Europe.[170] Moreover, I embrace the understanding of the complementarity

---

[162] European Commission (2014), *COM (2014) 158 final*, 3.

[163] A list of rule of law-related indexes and indicators is in Pech (2013), *Rule of Law as a Guiding Principle of the EU's EA*. Documents endorsing the rule of law include: United Nations, Secretary General, *The Rule of Law and Transitional Justice in Conflict and Post-conflict Societies. Report of the Secretary-General to the Security Council* (S/2004/616, 2004); United Nations, General Assembly, *Declaration on Principles of International Law Friendly Relations and Co-Operation among States in Accordance with the Charter of the United Nations* (1970); OSCE, Office for Democratic Institutions and Human Rights, 'ODIHR and the Rule of Law' <http://www.osce.org/odihr/103448>. OECD, Development Assistance Committee (DAC), *Security System Reform and Governance* (DAC Guidelines and Reference Series, 2005). See also at http://www.un.org/en/ruleoflaw/index.shtml.

[164] European Commission (2014), *COM (2014) 158 final*. European Commission, *Annexes to the Communication A new EU Framework to Strengthen the Rule of Law* ((Communication) COM (2014) 158 final, 2014).

[165] Discussed in Pech (2009), *The Rule of Law as a Constitutional Principle of the European Union*.

[166] The European Commission participates as an observer in the works of the Venice Commission.

[167] Council of Europe, European Commission for Democracy through Law (Venice Commission), *Report on the Rule of Law* (Study No 512/2009, 2011). Internet paper. The Council of Europe and the Rule of Law - An overview - CM(2008)170, 21 November 2008.

[168] Council of Europe, *Memorandum of Understanding between the Council of Europe and the European Union CM(2007)74 1* (117th Session of the Committee of Ministers, 2007) Article 10. According to Angelini, the EU law acts as a mezzanine between national constitutional traditions and the CoE, thus performing "a connection and catalyst of homogeneity between the other two". Angelini (2007), p. 165.

[169] Angelini (2007).

[170] Committee of Ministers of the Council of Europe, *The Council of Europe and the Rule of Law - An Overview, CM (2008) 170 (CoE and the Rule of Law)* (2008).

between substantive and procedural rule of law principles expounded by Kilpatrick[171] (and Waldron[172]).

The first tenet is "legality, which implies a transparent, accountable, democratic and pluralistic process for enacting laws (supremacy of the law)."[173] It is a fundamental principle[174] and overarching tenet[175] that testifies to the connection between the rule of law and the other values-principles listed in article 2 TEU, such as the principle of democracy, which constitutes "one of the foundations of the European Union".[176] Indeed, legality has a 'thin' meaning, i.e. supremacy of the law, and a thick one, which consists in the procedures that must be followed in order to consider law supreme. At the same time, the principle of democracy does not exhaust itself in legality; it has strong connections with legal certainty as well as equality and non-discrimination.

The second tenet is legal certainty, which corresponds to the general principle of legal certainty and protection of legitimate expectations.[177] This tenet requires both the existence of a legal basis to enable the actions of a state and its organs, and the conformity of said legal basis with parameters of quality guaranteeing foreseeability and the protection of legitimate expectation, "by virtue of which the effect of…legislation must be clear and predictable for those who are subject to it",[178] so as to enable them to regulate their conduct. Rules must be "formulated with sufficient precision to enable the citizen to adjust his conduct accordingly, and so compl[y] with the requirement of foreseeability laid down in the case-law of the ECtHR."[179] Indeed, the ECtHR has progressively identified the criteria of quality of the law (chapter 6, section 3),[180] e.g. it must be made known before implementation and be easily accessible. While this does not exclude recourse to secrecy (as a first order issue), rules

[171] Claire Kilpatrick, 'On the Rule of Law and Economic Emergency: the Degradation of Basic Legal Values in Europe's Bailouts' (2015) 35 Oxford Journal of Legal Studies p. 325.
[172] Rule of law and legality are often used as synonyms. Jeremy Waldron, 'The Concept and the Rule of Law' (2008) 43 Georgia Law Review 1.
[173] European Commission (2014), *COM (2014) 158 final*, p. 4.
[174] Judgment of 29 April 2004 in Commission v. CAS Succhi di Frutta, C-496/99 P, EU:C:2004:236, para 63: "the fundamental principle that, in a community governed by the rule of law, adherence to legality must be properly ensured".
[175] Waldron (2008), 'The Concept and the Rule of Law'.
[176] Judgment of 9 March 2010 in European Commission v. Federal Republic of Germany, C-518/07, EU:C:2010:125, para 41.
[177] Tridimas (2006), *The General Principles of EU Law*.
[178] Judgment of 12 November 1981 in Meridionale Industria Salumi and Others, Joined cases 212 to 217/80, EU:C:1981:270, para 17; Council of Europe (2011).
[179] Judgment of 20 May 2003 in Österreichischer Rundfunk and Others, Joined cases C-465/00, C-138/01 and C-139/01, EU:C:2003:294, para 77.
[180] For a summary, see Council of Europe (2013); Council of Europe (2011).

enabling a resort to secrecy should be publicly debated (the second order issue).[181] As AG Saugmandsgaard Øe noted in *Tele2 Sverige*,[182] the ECJ has listed for the first time some parameters of lawfulness in *WebMindLicenses*, where the Court held that "the law must be sufficiently clear and precise" and that the limitations imposed upon the rights afford "legal protection against any arbitrary interference" by public authorities (§ 81).[183] AG Saugmandsgaard Øe argues that the expression "provided for by law" in EU law should be understood as susbstantively as the reading given by the ECHR (§ 140 of his opinion), since the protection afforded in the EU cannot be lower than that provided in the ECHR. The rationale of lawfulness is to "respect the ordinary citizen as active centers of intelligence",[184] who do not simply obey, but interact and, if need be, can challenge the legal process.

Third, the "prohibition of arbitrariness of the executive powers"[185] protects against arbitrary or disproportionate intervention,[186] thus including the general principle of proportionality.[187] While it is understood that executive powers may require a margin of flexibility,[188] particularly at times of emergency as discussed in these pages, discretion cannot be unfettered, and conduct must conform to fairness, reasonabless, rationality and inclusion.[189] This ideally extends to the activities of intelligence services.[190] Hence, the scope of discretionality must be carved out in law and accompanied by minimum safeguards,[191] and at the same time it must be exercised proportionally, and "where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference".[192] The same is the case whenever Member States act within the scope of EU law. Such limit is fundamental for a substantive

[181] Deirdre Curtin, 'Overseeing Secrets in the EU: A Democratic Perspective' (2014) 52 Journal of Common Market Studies.
[182] Opinion of AG Saugmandsgaard Øe of 19 July 2016 in Tele2 Sverige and Watson and others, Joined cases C-203/15 and C-698/15, EU:C:2016:572.
[183] Judgment of 17 December 2015 in WebMindLicenses, C-419/14, EC:C:2015:832.
[184] Waldron (2008), 'The Concept and the Rule of Law', p. 57.
[185] European Commission (2014), *COM (2014) 158 final*, p. 4.
[186] Judgment of 21 September 1989 in Hoechst v. Commission, Joined cases 46/87 and 227/88, EU:C:1989:337, para 19.
[187] Tridimas (2006), *The General Principles of EU Law*.
[188] E.g. the proposal made in *Joined cases C-203/15 and C-698/15 - Opinion of AG Saugmandsgaard Øe*, para 237.
[189] Council of Europe (2011), para 52.
[190] Fundamental Rights Agency (2015). See also the recommendations contained in Article 29 Data Protection Working Party (2014).
[191] Judgment of 8 April 2014 in Digital Rights Ireland and Seitlinger and Others, Joined cases C-293/12 and C-594/12, EU:C:2014:238, para 54.
[192] Ibid, para 47.

understanding of the rule of law, and goes hand in hand with the availability of independent and impartial courts.

The tenet of independent and impartial courts is a precondition for the general principle and rights of defence.[193] Independent and impartial courts require the judiciary to be a separate power, i.e. not controlled by other governmental authorities (typically the executive), and not subject to external pressure, such as "political influence or manipulation". [194] Independent and impartial courts give substance to the rights of defence through the fifth tenet, effective judicial review,[195] including respect for fundamental rights. As the court recalls in *Schrems*, "The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law."[196] Such a tenet corresponds to the general principle of effectiveness and fundamental rights. Review includes administrative acts, and is crucial if serious consequences on rights and interests are at stake.[197] Review cannot be bypassed by amending or replacing a decision under scrutinity "in the course of the proceedings in order to deprive the other party of the possibility of extending its original claims and pleas to the later decision or of presenting additional claims and pleas against it."[198] Judicial review includes verifying whether the evidence upon which a decision is founded "has been obtained and used in breach of the rights guaranteed by EU law and, especially, by the Charter" to the extent that… "If that requirement is not satisfied and, therefore, the right to a judicial remedy is not effective, or if another right guaranteed by EU law is infringed, the evidence obtained…must be disregarded and the contested decision which is founded on that evidence must be annulled if, as a result, the decision has no basis."[199]

Fundamental rights are not only general principles of EU law (art. 6 (3) TEU) whereof the Court ensures observance,[200] but a principle of the rule of law fully embraced by the EU after

[193] Tridimas (2010), 'Primacy, Fundamental Rights and the Search for Legitimacy'.
[194]The notion of independence in the context of Data Protection Authorities is discussed in chapter 7.
[195] For all requirements of access to justice, see Council of Europe (2011), para 53-58.
[196] Judgment of 6 October 2015 in Schrems, C-362/14, EU:C:2015:650, para 95.
[197] Judgment of 18 January 2007 in PKK and KNK v. Council, C-229/05 P, EU:C:2007:32, para 109.
[198] Judgment of 12 March 2014 in Al Assad v. Council, T-202/12, EU:T:2014:113, para 33.
[199] *C-419/14 - WebMindLicenses*, paras 87-89.
[200] Judgment of 14 May 1974 in Nold KG v. European Commission, C-4/73, EU:C:1974:51, para 13; Tridimas (2010), 'Primacy, Fundamental Rights and the Search for Legitimacy'.

the entry into force of the Lisbon Treaty, as testified to by article 2 TEU. Fundamental rights are now enshrined in the Charter, which, thanks to article 6 (1) TEU,[201] enjoys a status analogous to that of a constitutional Bill of Rights within a nation state,[202] and which established clear rules for permissible limitations, to be found in article 52 of the Charter. Respect for fundamental rights means that their enjoyment must be as complete as possible, and that limitations pertain to the exercise of those rights, rather than their guarantees. Article 52 (1) of the Charter authorizes the limiting of qualified rights only if necessary either to pursue objectives of general interest recognized by the Union, or to protect the substance of the rights of others.[203] Pursuant to article 52 (3) of the Charter, whenever rights protected by the Charter correspond to those safeguarded by the ECHR, the grounds for permissible limitations listed therein should apply (see chapters 6 and 7). Such grounds are often associated with an emergency, as described above, and are usually considered part of the notion of material *ordre public*. The grounds for permissible limitations found in both the Charter and the ECHR contain rigorous guarantees to prevent arbitrariness by public authorities: necessity (vis-à-vis a democratic society), proportionality, and the respect of the essence of the right. In other words, rights are protected by the ideal *ordre public* as general principles and part of the constitutional architecture, while material *ordre public* can constitute a limitation on their exercise, but not their guarantees. In the context of the refusal of Austria to recognize the acquired surname of one of its nationals that indicated nobility, the Court followed its previous jurisprudence [Case C-36/02 Omega § 30, Case C-33/07 Jipa § 23]:

> *"The Court has repeatedly noted that the concept of public policy as justification for a derogation from a fundamental freedom must be interpreted strictly, so that…public policy may be relied on only if there is a genuine and sufficiently serious threat to a fundamental interest of society…and only in so far as those objectives cannot be attained by less restrictive measures. … It is not indispensable for the restrictive measure issued by the authorities of a Member State to correspond to a conception shared by all Member States as regards the precise way in which the fundamental right or legitimate interest in question is to*

[201] Since Article 6 in the Treaty of Maastricht read "the Union is founded on the principles of…", some scholars believe the new wording of art. 2 TEU is a retrenchment of the constitutional safeguards afforded by EU primary law. Tridimas (2010), 'Primacy, Fundamental Rights and the Search for Legitimacy'. See also *supra,* footnote n. 146.

[202] Rodotà (2012).

[203] Objectives of general interest arguably fulfil the aims identified in article 3.1 TEU ("the promotion of peace, the preservation of its traditions and citizens' well-being,"), notably the AFSJ (3.2), the internal market (3.3), including scientific and technological advance, the economic and monetary Union (3.4), and external relations reflecting its own internal values (3.5).

be protected and that, on the contrary, the need for, and proportionality of, the provisions adopted are not excluded merely because one Member State has chosen a system of protection different from that adopted by another State."[204]

The final tenet, equality before the law,[205] corresponds both to the general principles and rights of equality and non-discrimination,[206] prohibiting unequal treatment of certain categories of individuals, to the effect that cases may not be decided incoherently and unfairly. In a substantive understanding of the rule of law,[207] non-discrimination can be seen as entailing participation in decision-making,[208] and, relatedly, potential "*ex ante* and *ex post* legislative evaluation."[209]

Summing up, my critique of a simplistic trade-off (and, relatedly, deference) thesis derives from both an adherence to the paradigm of the rule of law, and the full integration of fundamental rights into the fabric of EU law, including in the AFSJ, as I discuss next.

2.3.2 THE RULE OF LAW IN THE AFSJ AND THE NATIONAL SECURITY EXCEPTION

The three objectives of general interest listed in article 3(1) TEU presuppose the reconciliation of security and rights.[210] Indeed, the 'constitutional' conception of security is instrumental to the pursuit of a society wherein fundamental rights are fully enjoyed, and is in line with the tenets of the rule of law. Such a constitutional conception of security and rights

[204] Judgment of 22 December 2010 in Ilonka Sayn-Wittgenstein v. Landeshauptmann von Wien, C-208/09, EU:C:2010:806, paras 86 to 91.
[205] Council of Europe (2011), para 65.
[206] Article 19 TFEU, which repealed article 13 ECT, has a different scope than article 21 of the Charter, in that it enables the EU to adopt any measures to combat clearly enumerated grounds of discrimination. No such power is created by article 21 of the Charter; in turn, article 21 does not affect the scope and aim of article 21. Another source of non-discrimination is article 11 of the Convention on Human Rights and Biomedicine as regards genetic heritage. Explanations Relating to the Charter of Fundamental Rights, OJ C 303/02 (Explanations to the Charter).
[207] For a discussion on New Governance in relation to the rule of law, see Kilpatrick (2015).
[208] United Nations, High Commissioner for Human Rights (OHCHR), *Human Rights Indicators. A Guide to Measurement and Implementation* (HR/PUB/12/5, 2012); Joana Mendes, *Rule of Law and Participation: A Normative Analysis of Internationalised Rulemaking as Composite Procedure* (Jean Monnet Working Paper Series, New York University School of Law, 2013); Maria Grazia Porcedda, 'The Manifold Significance of Citizens' Legal Recommendations on Privacy, Security and Surveillance' in Michael Friedewald, J. Peter Burgess, Johann Čas, Rocco Bellanova and Walter Peissl (eds), *Surveillance, Privacy and Security. Citizens' Perspectives* (Routledge fortchoming (2017)).
[209] Council of Europe (2011), para 51.
[210] Koen Lenaerts, 'The Basic Constitutional Charter of a Community Based on the Rule of Law' in Poiares Maduro and Azoulai (eds), *The Past and Future of EU Law* (2010); von Bogdandy (2010).

has found substance, first and foremost, in the creation of the Area of Freedom, Security and Justice (hereafter AFSJ), an internal, borderless area, protecting citizens' fundamental rights, guaranteeing a high level of security, and fostering access to justice, with respect for the different legal systems and traditions of Member States (articles 3(2) TEU and 67 TFEU).[211]

The fact that the Lisbon Treaty brought the AFSJ under the full remit of EU law[212] and its "normal system of jurisdiction"[213] enables the institutions to pursue both security and fundamental rights. Having said that, I agree with Monar[214] that a common law-type approach is needed to interpret the meaning of the AFSJ: relevant Treaty provisions must be accompanied by policy documents. From that perspective, the application of the rule of law – and particularly fundamental rights obligations – to the AFSJ appears more nuanced. However, this may be the consequence of the legacy of intergovernmentalism, and the ensuing reluctance of pooling competences, that affects the AFSJ, rather than the wish to privilege security over liberties. In this respect, Carrera and Guild[215] noted how the European Council's strategic guidelines adopted in June 2014[216] pursuant to article 68 TFEU seem to attempt the 'de-Lisbonising' of the AFSJ, by means of overlooking the fundamental rights and rule of law obligations, for the sake of bringing the AFSJ back under a pure intergovernmental logic. The authors show how the different programmes sponsored by the relevant institutional actors – Commission, Parliament, Council and European Council – are at odds with one another.

When it comes to institutional arrangements, all AFSJ-related initiatives are subject to checks for compliance with the rule of law. All new Commission initiatives must undergo mandatory impact assessments that include an appraisal of which fundamental rights are affected, and to what extent,[217] as well as whether the envisaged interferences are

[211] Craig and de Búrca (2015).
[212] Piris (2010); Paul Craig, *The Lisbon Treaty, Revised Edition: Law, Politics, and Treaty Reform* (Oxford University Press 2013). On criminal law, see Ester Herlin-Karnell, 'EU Competence in Criminal Law after Lisbon' in Andrea Biondi, Piet Eeckhout and Stefanie Ripley (eds), *EU Law after Lisbon* (Oxford Scholarship Online 2012). In general, Steve Peers, *EU Justice and Home Affairs Law* (Oxford University Press 2011).
[213] Francis G. Jacobs, 'The Lisbon Treaty and the Court of Justice' in Andrea Biondi, Piet Eeckhout and Stefanie Ripley (eds), *EU law after Lisbon* (Oxford Scholarship Online 2012), p. 203.
[214] Joerg Monar, 'The Area of Freedom, Security and Justice' in Armin von Bogdandy and Jürgen Bast (eds), *Principles of European Constitutional Law* (Hart Publishing 2009).
[215] Sergio Carrera and Elspeth Guild, *The European Council's Guidelines for the Area of Freedom, Security and Justice 2020: Subverting the 'Lisbonisation' of Justice and Home Affairs?* (CEPS Essay n° 13/14, 2014).
[216] *European Council, Conclusions, 26/27 June 2014, EUCO 79/14* (2014). European Commission, *An Open and Secure Europe: Making it Happen* ((Communication) COM (2014) 154 final {SWD(2014) 63 final}, 2014).
[217] European Commission, *Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union* ((Communication) COM (2010) 573/4, 2010); European Commission, *Compliance with the Charter of Fundamental Rights in Commission legislative proposals. Methodology for systematic and rigorous*

necessary.[218] Whenever the proposal introduces a limitation pursuant to article 52 of the Charter, or represents a tool to promote or implement a particular right, the preamble of the text includes recitals formally declaring compliance with the Charter. In such instances a summary of the findings of the legality check, vis-à-vis the Charter, must be included in the explanatory memorandum.

Moreover, the Commission is committed to fostering a cross-institutional "fundamental rights culture", whereby rights provide both guidance for, and limitations to, the Union's activities.[219] Accodingly, in its Communication 'the European Agenda on Security', the Commission asserted that "security and respect for fundamental rights are not conflicting aims, but consistent and complementary policy objectives", and that it would "strictly test that any security measure fully complies with fundamental rights whilst effectively delivering its objectives".[220] Consequently, ensuring the respect of fundamental rights and the tenets of the rule of law would appear to be the Commission's top priority.

Having said that, it is crucial to appraise the effective weight of the national security exception (including maintaining law and order), which is, according to article 4(2) TEU and 72 TFEU (where the adjective used, however, is 'internal'), the sole responsibility of Member States, anchoring national security and law and order firmly outside the scope of EU law. According to Hinarejos,[221] article 72 does not innovate greatly. It could be seen as both providing grounds for derogating from EU law, and an additional limitation of EU competences. In practice, the CJEU would retain the power to check the compatibility of a

---

monitoring ((Communication) COM (2005) 172 final, 2005). For an updated list of documents and guidelines, see: http://ec.europa.eu/smart-regulation/index_en.htm. / Better Regulation Action Plan [COM(2002) 276 final.] (http://ec.europa.eu/governance/impact/iab/iab_en.htm).

[218] Although the outcome is not binding, the assessment is additional to the Legal Service's check of conformity of proposed draft acts with the Charter. The Legal Service is in particular supposed to liaise with the Group of Commissioners on Fundamental Rights, Anti-discrimination and Equal Opportunities.

[219] European Commission (2005), *COM (2005) 172 final*; European Commission (2010), *COM (2010) 573/4*. Annual Reports on fundamental rights in the domestic and external action are also part of this approach: European Commission, *Report on the Practical Operation of the Methodology for a Systematic and Rigorous Monitoring of Compliance with the Charter of Fundamental Rights* ((Communication) COM (2009) 205 final, 2009). Members of the European Commission pronounce before the Court of Justice a solemn undertaking to respect the Charter. The Commission undertook to monitor the compliance with the Charter of the two legislative branches, and to initiate annulment proceedings before the Court of Justice if fundamental rights are infringed. Likewise, the Commission will file a procedure for action for failure to fulfil an obligation, whenever the transposition of a EU law by a Member State violates provisions on fundamental rights.

[220] European Commission, *The European Agenda on Security* ((Communication) COM(2015) 185 final, 2015), p. 3.

[221] Alicia Hinarejos, 'Law and Order and Internal Security Provisions in the Area of Freedom, Security and Justice: Before and After Lisbon' in Christina Eckes and Theodore Konstadinides (eds), *Crime within the Area of Freedom, Security and Justice: a European Public Order* (2011).

national action in conflict with a rule of EU law, provided such action would not entail a "fundamental policy choice" [222] (so as not to exceed its boundaries of competence).

The exception extends to judicial review. Accordingly, the CJEU "shall have no jurisdiction to review the validity or proportionality of operations carried out by the police or other law-enforcement services of a Member State or the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security" in the context of operations of judicial cooperation in criminal matters and police cooperation in the AFSJ. While Jacobs judges the exception contained in article 276 TFEU "of rather limited scope",[223] for Hinarejos[224], it represents the real change. She notes that it is unfortunate that the caveat "where such action is a matter of national law", contained in the Constitutional Treaty, has been removed from the wording of article 276 TFEU. The CJEU may be prevented from carrying out both direct (infringement procedure) and indirect (preliminary ruling) controls on Member States' actions, even if such actions constitute the implementation of EU law, as is likely under chapters 4 and 5 of title V TFEU. Moreover, it has to be understood the extent to which article 276 TFEU may have implications for the scope of application of the Charter, which should be respected also when Member States derogate from EU law[225] (*infra*, section 2.4).

According to Hinarejos, the only way to avoid injustice is by fostering greater cooperation between the CJEU and national courts. Admittedly, an extra layer of judicial review would reinforce the rule of law, but ultimately what matters is the availability of judicial review by impartial and independent courts. The national security exception could thus be seen as a form of deference to national courts, but in a spirit of cooperation,[226] since the latter are the day-to-day executor of national and EU law (also in the light of article 19 (1) TEU), and the ECtHR as a court of last resort (which has progressively defined the margin of manoeuvre of contracting parties to the ECHR in cases of national security exceptions[227]). This would reinforce the idea of a European *ordre public,* where different levels perform different functions. Undeniably, understanding the extent to which national, or rather internal, security can be seen as falling outside the scope of EU law, whenever it relies on an instrument of EU

[222] Ibid.
[223] Jacobs (2012), p. 203.
[224] Hinarejos (2011).
[225] Craig (2013); Hinarejos (2011).
[226] Koen Lenaerts, 'The Contribution of the European Court of Justice to the Area of Freedom, Security and Justice' (2010) 59 International and Comparative Law Quarterly, p. 255.
[227] Council of Europe (2013).

law – such as privacy-related instruments– is essential to disprove the practical application of the trade-off and deference theses, but it has to be done with reference to specific instruments, and this will be the object of chapters 3 and especially 4.

In light of this uncertainty, a glimmer of hope comes from the CJEU. In its landmark judgment on data retention, for the first time the Court invalidated a Directive adopted for the legitimate objective of fighting crime and terror, based on its failure to comply with fundamental rights and the rule of law.[228] What is more, the combined reading of the *Digital Rights Ireland*[229] judgment with *Schrems*[230] may suggest the EU is giving up internal market rigour in exchange for the authority to closely evaluate member states' conduct on matters of public security.[231] Mindful that one swallow does not a summer make, we may need more case law before we are able to draw a meaningful conclusion about the scope of the national security exception.

As an interim epilogue, it may not be unreasonable to envisage a continuation of clashes between European institutions, and a certain resistance of the European Council and Council of Ministers to a greater democratization of policy-making in this area, given the sensitivity of the subject-matter. The recent wave of terror attacks combined with the migration crisis could favour an unwelcome return to intergovernmental practices, and the attendant implication of a serious setback to the European *ordre public* as created by Lisbon. I discuss this in the next section, where I tackle the last criticism to the trade-off thesis, regarding times of emergency.

2.4 TIMES OF EMERGENCY AND NORMALIZATION

The last claim of Posner and Vermeule's trade-off thesis to be analysed is that security and liberty should be traded-off *at times of emergency*. This calls for a necessary analysis of the notion of emergency[232] and the powers conferred upon the Union in this respect, in order to see the extent to which emergencies can bend the application of the Union *ordre public* devised thus far.

[228] *Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*.
[229] Ibid.
[230] *C-362/14 - Schrems*.
[231] I owe this reflection to a fruitfuil discussion with my supervisor, Marise Cremona. All mistakes remain mine.
[232] For a reflection on the concept in comparative terms, see Dyzenhaus (2012).

To begin with, the Lisbon Treaty contains no 'emergency clause'[233] and very scant direct references to the word 'emergency',[234] which is never defined. According to secondary legislation, and particularly article 2, letter j, of Regulation 513/2014 on the establishment of the instrument for financial support for police cooperation,[235] 'emergency situation' means any security-related incident or newly emerging threat which has or may have a significant adverse impact on the security of people in one or more Member States. This definition of emergency underlines its unpredictability, and posits crisis, potential threat for security and indeterminacy as its constituent elements. Thus, the absence of a definition of emergency may well be intentional.

Accordingly, article 15 (3) TEU can be seen to confer emergency powers upon the European Council. Pursuant to article 15 (3) TEU, "when the situation so requires", a special meeting of the European Council can be convened, to provide the necessary impetus and define priorities (art 15(8) TEU), adopt decisions on the strategic interests and priorities concerning certain themes within the CFSP and external action (art 22 TEU), and define strategic guidelines within the AFSJ (art 68 TFEU). What is more, according to art 222(2) TFEU, the European Council "shall regularly assess the threats facing the Union in order to enable the Union and its Member States to take effective action".

Inasmuch as the acts adopted by the European Council produce legal effects *vis-à-vis* third parties, they are subject to a review of legality by the Court of Justice (art. 263 TEU). Moreover, the European Council shall defer all legislative initiative to the competent EU institutions, which are subject to a broader check of compatibility with "the Treaties, general principles of law and fundamental rights",[236] so that legality is properly ensured. For instance, it is the Council which makes arrangements for the implementation of actions taken pursuant to the solidarity clause (art 222 TFEU) and informs the Parliament.

[233] Kilpatrick (2015).
[234] Emergency is referred to in articles 30.2 TEU (CFSP) and 78.3 TFEU (asylum).
[235] Regulation 513/2014/EU of the European Parliament and of the Council of 16 April 2014 Establishing, as Part of the Internal Security Fund, the Instrument for Financial Support for Police Cooperation, Preventing and Combating Crime, and Crisis Management and Repealing Council Decision 2007/125/JHA, OJ L 150/93.
[236] *C-362/14 - Schrems*, para 60.

Hence, even at times of emergency in which the European executive can be lawfully in charge, the abovementioned tenets of the rule of law are fully working[237] (provided that the executive acts within the given boundaries).

To what extent does the scope of Union action and its competence vis-à-vis that of Member States in the context of emergencies matter? The Treaties contain a number of provisions that enable action to tackle crises "in the Member States which allow for EU action or controlled suspension of normally applicable rules",[238] or call for joint action (with the Council in the position of coordinator) and solidarity,[239] namely articles 196, 214 and 222 TFEU. The latter is the solidarity clause, which is relevant for the case study of cybersecurity, and reads

> *"1. The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to:*
> *(a) — prevent the terrorist threat in the territory of the Member States;*
> *— protect democratic institutions and the civilian population from any terrorist attack;*
> *— assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack;*
> *(b) assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster.*
> *2. Should a Member State be the object of a terrorist attack or the victim of a natural or manmade disaster, the other Member States shall assist it at the request of its political authorities. To that end, the Member States shall coordinate between themselves in the Council. …"*

Cremona[240] notes that pursuant to article 6 TFEU, the Union's intervention within the remit of the solidarity clause (as well as article 196 TFEU) is concretized in "actions to support, coordinate or supplement the actions of the Member States, without thereby superseding their competence in these areas" (art 2(5) TFEU). Hence, during an emergency the bulk of action falls on the shoulders of Member States. This does not entail the automatic irrelevance of the Union *ordre public* (or its irrelevance at all). Moreover, actions taken

[237] For a critical – but fair – appraisal of the failures of the Union/CJEU to upheld the rule of law *vis-à-vis* the economic emergency, see Kilpatrick (2015).
[238] Ibid., p. 328. In the context of economic policy, these are articles 122 and 143-144 TFEU.
[239] Marise Cremona, 'The EU and Global Emergencies: Competence and Instruments' in Antonio Antoniadis, Robert Schutze and Eleanor Spaventa (eds), *The European Union and Global Emergencies: A Law and Policy Analysis* (Hart Publishing 2011).
[240] Ibid.

pursuant to article 222(1) can and do overlap with measures of shared competence taken in the AFSJ, and viceversa.[241]

Emergencies are qualified by public policy (ideal *ordre public*), public security (law and order and national security) or public health determinations, which in turn constitute grounds allowing Member States to derogate from EU law (see *infra*). Examples are contained in articles 36, 45(3), 52 and 65 TFUE, and similarly to 'emergency', they are not described, because of the acceptability of different understandings of public policy in the Member States (e.g. *Van Duyn*[242], *Sayn-Wittgenstein, supra* section 2.3.1).[243]

When emergencies warrant initiatives toward objectives other than public security (viz. law and order and national security), Member States actions are likely to be firmly grounded in Union law, and thus must conform to the elements of its *ordre public*. In cases concerning public security, the situation is more nuanced due to the 'law and order and internal security' exception carved in article 4 TEU, and leads one to question whether such action falls outside the remit of Union *ordre public*, leaving Member States free to trade-off security with liberties at will.

In the first place, Member States may well be acting within the remit of Union law, as is the case when countering terrorism and cyberattacks, and therefore the national security exception would constitute derogation from EU law. According to settled case law,[244] whenever derogations concern human rights, they are to be interpreted restrictively. In *Rutili*, in the context of freedom of movement, the Court argued that exceptions cannot be found generically, but for specific conduct constituting "a genuine and sufficiently serious threat to public policy (§28)". Member States must "base their decision on the individual circumstances of any person under the protection of Community Law and not on general considerations (§29)."[245]

Moreover, following a broad interpretation of article 51 of the Charter, argued for instance by Craig,[246] 'implementing' EU law would mean 'falling within the scope of EU law', and hence the Charter should be respected also when Member States derogate from EU law.

[241] In fact, Cremona notes that initiatives in the field of counter-terrorsism include both solidarity and civil protection elements. Ibid.
[242] Judgment of 4 December 1974 in Van Duyn v. Home Office, C-41/74, EU:C:1974:133, para 18.
[243] On the subject matter, see Lenaerts (2010), 'The Contribution of the ECJ to the AFSJ'.
[244] As from *C-4/73 - Nold*.
[245] Judgment of 28 October 1975 in Rutili v. Ministre de l'intérieur, C-36/75, EU:C:1975:137.
[246] Craig (2013), p. 210 to 213.

Finally, the Court may well intervene to evaluate whether the Member State has exceeded the scope of its derogation. In practice, the CJEU would retain the power to check the compatibility of a national action in conflict with a rule of EU law, provided such action would not entail a "fundamental policy choice"[247] (*supra*, section 3.2.2).

In the second place, even if Member States were acting outside the remit of Union law, they would not operate in a legal void. On the one hand, they are constrained by their constitutions, which guarantee rights constituting the traditions common to the Member States and informing the general principles of Union law (art 6 (3) TEU). On the other hand, as the Court clarified, for instance in a reference for preliminary ruling on family reunification,[248] situations that are not covered by Union law are covered by the ECHR, which also guarantees rights, pursuant to art 6 (3) TEU, constituting general principles of Union law. The words of Dyzenhaus seem apt in this respect

> *"... it is possible for a virtuous rather than a vacuous cycle of legality to unfold as long as one sees that the challenge is not to decide on which institution or power should be the primary actor, but that the legislature, the executive and the judiciary have to participate together in a common constitutional project. We do not have to choose between a legislative, an executive, or a judicial model for dealing with emergencies. Rather, what we need is a normative framework for understanding how, in the light of experience, the grip of constitutional principles can be maintained."*[249]

In the case of the Union, this could be done at multiple levels. Following Angelini, the system enshrined in article 6 TEU constitutes a macro European *ordre public* that defines the *vouloir vivre* of the Members of the Union. Such *vouloir vivre* allows to make exceptions at times of emergency, but as recalled above, it is the exercise of rights, and not their guarantees, which can be constrained. A case in point is that on restrictive measures[250] following the

[247] Hinarejos (2011).
[248] "Thus, in the present case, if the referring court considers, in the light of the circumstances of the disputes in the main proceedings, that the situation of the applicants in the main proceedings is covered by European Union law, it must examine whether the refusal of their right of residence undermines the right to respect for private and family life provided for in Article 7 of the Charter. On the other hand, if it takes the view that that situation is not covered by European Union law, it must undertake that examination in the light of Article 8(1) of the ECHR." Judgment of 15 November 2011 in Dereci and others v. Bundesministerium für Inneres, C-256/11, EU:C:2011:734, para 72.
[249] Dyzenhaus (2012), p. 460.
[250] Council Regulation 881/2002/EC of 27 May 2002 Imposing Certain Specific Restrictive Measures Directed Against Certain Persons and Entities Associated with Usama bin Laden, the Al-Qaida Network and the Taliban, and Repealing Council Regulation (EC) No 467/2001 Prohibiting the Export of Certain Goods and Services to Afghanistan, Strengthening the Flight Ban and Extending the Freeze of Funds and Other Financial Resources in Respect of the Taliban of Afghanistan, OJ L 139. The text has been the object of a number of cases and related

much debated[251] *Kadi* saga.[252] The Court of Justice upheld a number of rule of law tenets in the face of the supposed imminent threat posed by individuals listed by the UN and subsequently the Council. Although the Court found that the restriction of the right to property was justified, in principle, in the light of the objective it intended to pursue (§ 366), such restriction was implemented in such a way as to deprive the person concerned of any guarantees of defence (§369), thus constituting an excessive interference with his right, which justified the annulment of Council Regulation 881/2002.

As De Búrca noted – praising the result for fundamental rights but not the substantive reasoning followed[253]– the ECJ showed limited if any deference towards the U.N. Security Council, and I may add the Council, which represent the 'executive' in this matter. And here I finally address the deference thesis, though in a somewhat frustrating manner, since I believe that it is not yet possible to carry out a fully-fledged evaluation as far as the Union is concerned. The high degree of institutional discontinuity of the EU hinders appraising the extent to which the judiciary has deferred the decision about 'striking the right balance' between security and liberties to the executive power,[254] though Curtin notes the CJEU's strict stance *vis-à-vis* the higher levels of deference showed by national and regional courts.[255] This last point brings to the fore the fact that the ECtHR possibly tends to defer more,[256] therefore the multilevel *ordre public* is an imperfect beast, but it still represents a multilevel

---

updates, available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002R0881&qid=1469203048156.

[251] For a comprehensive review of literature, see Sara Poli and Maria Tzanou, 'The Kadi Rulings: A Survey of the Literature' in Marise Cremona, Francesco Francioni and Sara Poli (eds), *Challenging the EU Counter-terrorism Measures through the Courts*, vol AEL 2009/10 (European University Institute Working Papers 2009). In general, Marise Cremona, Francesco Francioni and Sara Poli, *Challenging the EU Counter-terrorism Measures through the Courts* (European University Institute Working Papers, Academy of European Law 2009/10, 2009); Eleanor Spaventa, 'Counter-Terrorism and Fundamental Rights: Judicial Challenges and Legislative Changes after the Rulings in Kadi and PMOI' in Antonio Antoniadis, Robert Schutze and Eleanor Spaventa (eds), *The European Union and Global Emergencies: A Law and Policy Analysis* (Hart Publishing 2011).

[252] Particularly the ECJ's Judgment of 3 September 2008 in Kadi and Al Barakaat International Foundation v. Council and Commission, Joined Cases C-402/05 P and C-415/05, EU:C:2008:461 (Kadi I).

[253] She criticized the pluralist approach of the ECJ, which betrayed the EU's self-proclaimed tradition of adherence and engagement with the international community and its law, and argued that the same protective result could have been achieved with a soft constitutionalist approach following, for instance, the line of thinking pioneered by the German Constitutional court in the *Solange* cases. Gráinne de Búrca, *The European Court of Justice and the International Legal Order after Kadi* (Jean Monnet Working Paper 01/09, 2009).

[254] It should be recalled that, prior to the entry into force of the Lisbon Treaty, the ECJ had limited authority on fundamental rights, with the exception of interventions that could facilitate the establishment of the internal market (Advocate General Léger (2005)) due to the fact that the Charter was not legally binding. Second and more importantly, the ECJ could rule on issues strictly pertaining to EU law or the 'first pillar', and thus was not generally competent in the area of police and judicial cooperation disciplined in former Title VI of the Treaty on the European Union.

[255] Curtin (2009), *Executive power in the EU*, chapter 7 'Unitary Executive Power'.

[256] To this effect, ibid.

system of checks and balances to counter lopsided balancing and the threat of normalization, onto which I move now.

2.4.1 THE THREAT OF NORMALIZATION

In section 1 I noted that Posner and Vermeule's deference thesis does not take into account the duration of insecurity caused by an emergency. Although the notion of 'emergency' cannot be defined once and for all, the trade-off model stems from the fight against terrorism. Terrorism, unlike war, threatens survival in intermittent ways. Its open-endedness bears the danger of normalization, whereby what should have been temporary becomes the norm;[257] the longer the period of emergency, the more durable the subversion of normal procedures,[258] the deeper the potential damage to the rule of law tenets and, contextually, fundamental rights. Examples of measures adopted and maintained irrespective of the presence of an emergency are the Council decisions on counterterrorism,[259] the now invalidated[260] Data Retention Directive,[261] the Passengers Name Record data exchange,[262] the Transatlantic Finance Tracking Program (Swift) data exchange[263] and the PNR Directive.[264]

---

[257] See, for instance, the constant extension of 'emergency' in France. Jean-Baptiste Jacquin, 'L'impossible Sortie de l'Etat d'Urgence' *Le Monde* (Paris, 2 January 2016). Hélène Bekmezian, 'L'Etat d'Urgence Prolongé pour Six Mois par l'Assemblée Nationale' *Le Monde* (Paris, 19 July 2016).

[258] Jenkins (2014).

[259] Council Framework Decision 2002/475/JHA of 13 June 2002 on Combating Terrorism, OJ L 164; Council Framework Decision 2008/919/JHA of 28 November 2008 Amending Framework Decision 2002/475/JHA on Combatting Terrorism, OJ L 330 (Framework Decision on Terrorism).

[260] *Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*.

[261] 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 105/54 (Data Retention Directive).

[262] Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the Signing, on Behalf of the European Union, of an Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement). For a brief summary of the PNR saga, see Matteo Bonfanti, Gloria González Fuster and Maria Grazia Porcedda, 'European Union' in Privacy International (ed), *Global Surveillance Monitor* (2011). On the *quid pro quo* surrounding the PNR data exchanges see Andrew Rettman, 'Security Fears Prompt US Scrutiny of EU Visa Waiver' *Eu Observer* (23 February 2015).

[263] Council Decision 2010/16/CFSP/JHA of 30 November 2009 on the Signing, on behalf of the European Union, of the 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 Purposes of the Terrorist Finance Tracking Program, OJ L 8 (TFTP Agreement). A brief account of the SWIFT affair can be found at Bonfanti, González Fuster and Porcedda (2011).

The rationale of such instruments becomes ingrained in the political system and informs policy-making also in areas of criminal law that do not represent an existential threat to the survival of society. This includes normalizing two features of the current fight against terrorism: the **expansion of the scope of criminal law** to include a broader understanding of unacceptable behaviour, the idea being to prevent 'risks' resulting from the intention of individuals;[265] and **intelligence-led policing, which seeks to identify 'typical' risky individuals** through profiling and surveillance.

As for the first feature, the scope of criminal law is expanded by attaching criminalization to inchoate offences, i.e. the preparatory phases of a recognized substantive offence "prior to and irrespective of the commission of any harm."[266] Traditional inchoate offences include attempt, conspiracy and incitement, which are sanctioned only for the most serious crimes and thus constitute the exception. The wide criminalization of inchoate offences stems from the belief that preparatory acts demonstrate the intention of the individual to offend (*mens rea*), and that society will benefit more from the offender being tackled at the root, since terrorism's *iter criminis* (the passage from attempt to action) is fast.[267] This challenges the criminal law principle of harm, turns the exception into the rule, and risks nullifying traditional due process and the burden of proof.[268] The extreme consequence consists in the normalization of what were originally temporary measures of material *ordre public* (administrative and secret policing and the use of discretionary power) to preserve the ideal *ordre public*. But the conflation of the two notions is typical of illiberal regimes, and the analogy cannot be silenced. A number of NGOs recently criticized the European Parliament's Civil Liberties Committee (LIBE) on the vague references to 'preparatory acts'[269] contained in the draft Directive on counter-terrorism.

Tackling inchoate offences calls for prevention, and naturally requires attempting to identify individuals susceptible to committing crimes, which are singled out on the basis of a

---

[264] Directive 2016/681/EU of the European Parliament and of the Council of 27 April 2016 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime, OJL 119 (PNR Directive).
[265] Ulrich Beck, 'La société du risque globalisé revue sous l'angle de la menace terroriste' (2003) 114 Cahiers internationaux de sociologie, p. 22.
[266] Sugman Stubbs and Galli (2012).
[267] Ibid.
[268] Ibid.
[269] Amensty International and Open Society Foundations International Commission of Jurists, *Joint Statement: After a Fast-track Process the European Parliament Takes a Troubling Position on Counter-terrorism in Europe* (2016) <http://www.amnesty.eu/content/assets/Joint_Statement_on_Counter-Terrorism_Directive_after_LIBE_vote__July_2016.pdf>.

profile of the potential offender. In other words, addressing inchoate offences hinges on preventive, intelligence-led and technology-assisted policing (often online), the second common feature of counterterrorism mentioned above. Intelligence-led policing stems from the increasing lack of effectiveness, or unavailability, of traditional police methods (e.g. victims reporting crime), partly caused by the blurring of law and order issues with national security issues.[270] While traditional policing is mostly reactive and overt, intelligence-led policing entails preventive, covert actions[271] and reliance on open source or privately generated 'intelligence', i.e. information stemming from personal data or from direct monitoring of individuals through new technologies,[272] typically related to the Internet, to stop the inchoate offenders, or to simulate the possibility to control the uncontrollable.[273] The monitoring can assume different forms, and is usually subsumed under the umbrella of 'surveillance'.[274] This stands in contrast with surveillance as a traditional instrument to enforce norms.[275] The great reliance on the use of "monitoring of persons, places, items, means of transport, flows of information"[276] (personal data processing), whether performed by individuals or machines, means that contemporary ways of tackling (potential) crimes rest heavily on sacrificing 'privacy'. The slogan "if you have done nothing wrong, you have nothing to hide",[277] is used to justify deeper interferences with 'privacy' than those legally permissible for the sake of security, or, otherwise said, the security versus privacy trade-off.

If Posner and Vermeule's model does not openly endorse the normalization of counterterrorism, it nonetheless overlooks the importance of the duration of emergency and

---

[270] Iain Cameron, *De Lege. National Security and the European Convention on Human Rights* (Iustus Förlag 2000).
[271] Ibid.
[272] European Group on Ethics in Science and New Technologies, *Ethics of Security and Surveillance Technologies. Opinion n. 28* (2014); Beck (2003); Huysman (2006); Tony Monahan, *Surveillance and Security. Technological Politics and Power in Everyday Life* (Routledge 2006); Unabhaengiges Landeszentrum fuer Datenschutz (ULD), *Report on Surveillance Technology and Privacy Enhancing Design* (SurPRISE Project Deliverable D 3.1, 2013); Céline Cocq and Francesca Galli, *The use of surveillance technologies for the prevention and investigation of serious crimes* (SURVEILLE Project Deliverable D 4.1 2012); Maria Grazia Porcedda, *Paper Establishing Classification of Technologies on the Basis of their Intrusiveness into Fundamental Rights* (SURVEILLE Project Deliverable D 2.4, European University Institute 2013).
[273] Beck (2003).
[274] Iriss Project Consortium, 'Surveillance, Fighting Crime and Violence (Iriss Project Deliverable D 1.1 2012); Kevin D. Haggerty and Amber Gazso, 'Seeing Beyond the Ruins: Surveillance as a Response to Terrorist Threats' (2005) 30 Canadian Journal of Sociology 169-187; United Kingdom, House of Lords, *Surveillance: Citizens and the State* (House of Lords Select Committee on the Constitution, 2009).
[275] Alan Westin, *Privacy and Freedom* (Atheneum Press 1967).
[276] This is part of the definition of surveillance of the SURVEILLE Project Consortium, *Description of Works of the SURVEILLE Project. Surveillance: ethical issues, legal limitations and efficiency* (Seventh Framework Programme, European Union 2011), p. 5. See *infra*, footnote n. 693.
[277] Daniel Solove, 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review 745.

cases of abuse. Contrary to Posner and Vermeule's claim that cases of abuses are limited, experience shows otherwise,[278] partly because of the new trends in preventive policing described just now. The use of discretionary powers inherent in the trade-off model affects both the exercise of liberties, and the guarantees attached thereto, to the extent that they may be interfered with to the point of obliteration. The reports of Amnesty International and Human Rights Watch[279] on the abuses perpetrated under the state of emergency in France are just the latest example. Leaving the executive room for manoeuvre to trade-off security with rights has sadly meant the crushing of absolute rights, i.e. rights that are not legally encroachable (such as the right to life, or the prohibition of torture[280]). In France, after the November attacks, this has meant tabling the discussion of stripping those condemned for terrorism of their French citizenship,[281] a measure notably used by Italian Fascism against its political opponents.

Recourse to discretionary measures increases the risk of arbitrariness and abuse by those implementing them, typically security forces, which are the hallmark of illiberal regimes against which the European *ordre public* has been built. Additionally, it means superseding internationally recognized standards on human rights, always in force in accordance with the principle of legality, ultimately disregarding the states' positive and negative obligations to respect, protect and fulfil human rights. Decision-making by the executive, as opposed to parliament, even if the government has been elected by citizens, compresses participation and thus democracy, which is one of the objectives of the European *ordre public,* and a continuous teleological objective of and within the Union.

Signing such a blank sheet in favour of the executive would mark an authoritarian turn against the values and principles constituting the *ordre public* of the Union, as well as the plea to respect the constitutional identities of Member States as recognised in article 4 TEU. This is where the importance of the AFSJ comes into play, beyond the national security exception, and why, in order to defy the trade-off beyond normative arguments, it is necessary to

[278] Scheinin (2009), *Terrorism and the Pull of 'Balancing'*; Scheinin (2009), *Report on Human Rights and Fundamental Freedoms while Countering Terrorism*. As for abuse of access to data, see *Joined cases C-203/15 and C-698/15 - Opinion of AG Saugmandsgaard Øe*, para 260.
[279] Amnesty International, *Des Vies Bouleversées. L'Impact Disproportionné de l'Etat d'Urgence en France* (Londres, 2016); Human Rights Watch, *France: Abus Commis dans le Cadre de l'Etat d'Urgence. Les Perquisitions Administratives et les Assignations à Résidence sans Autorisation Judiciaire Doivent Cesser* (3 February, 2016).
[280] On the point, see Cassese (2012), *I diritti umani oggi*; Scheinin (2009), *Report on Human Rights and Fundamental Freedoms while Countering Terrorism*.
[281] Bastien Bonnefous and Thomas Wieder, 'Hollande Confirme la Déchéance de Nationalité' *Le Monde* (Paris, 2 January 2016).

scrutinize measures adopted pursuant to title V TFEU. I will come back to this point in chapters 3 and 4, after having defined the methodological challenge in the next chapter. Before concluding, I address one last point, namely the supposed desire of citizens to trade-off liberties for enhanced security at times of emergency.

2.5 A FINAL REFLECTION: CITIZENS' FEELING OF INSECURITY AND APPROACH TO TRADE-OFF[282]

A final reflection, which does not stem from Posner and Vermeule's thesis, concerns the commonplace assumption that citizens would be ready to accept the trade-off in the name of security. Pursuant to council Decision 2009/902/JHA[283] and Regulation 513/2014, crime prevention includes measures that are intended to both reduce and otherwise contribute to reducing crime and citizens' feeling of insecurity. Often recourse to the trade-off is justified by the idea that this meets citizens' expectations, further corroborating the efficiency of the measures. Sacrificing liberties would therefore fulfil the principle of democracy, in that it would take into account citizens' desires.

Empirical research has been conducted which has directly involved citizens by means of participatory and deliberative events,[284] in order to investigate their acceptance of the use of so-called "surveillance-orientated security technologies"[285] and of the trade-off model. Such research produced interesting results. Citizens framed security in terms of safety and their top priority was freedom from petty crime. They would only support security measures perceived

[282] This section is based on the direct experience of the author as a member of the SurPRISE project and organizer of the large-scale and small-scale events.

[283] Council Decision 2009/902/JHA of 30 November 2009 Setting up a European Crime Prevention Network (EUCPN) and repealing Decision 2001/427/JHA, OJ L 321; Regulation 513/2014/EU on the Instrument for Financial Support for Police Cooperation.

[284] Twelve large-scale participatory events were carried out in Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland and the United Kingdom between January and March 2014. Five small-scale events were carried out in Denmark, Hungary, Italy, Spain and Norway in June 2014. The timing was set in the Document of Works, and therefore it is not possible to understand the extent to which the Snowden revelations had an impact on citizens' perceptions.

[285] They involved three technologies that differ in terms of perception of intrusiveness and proximity: easily visible and "detached" in the sense that the individual does not carry it and can, to some extent, hide from it (Smart CCTV); visible if the person pays attention to it, and "detacheable" in the GPS component (Smartphone location-tracking), but also useful due to apps; invisible and undetacheable from one's activities (Deep packet inspection), and hence more pervasive, also because behavioural advertising may not be seen as beneficial. The small scale event featured the addition of biometrics and drones.

as efficient in achieving such goals, notably in relation to experience.[286] Citizens argued national security to be a remote concept potentially used for scapegoating, and insisted heavily that any measures of surveillance should be complemented by adequate safeguards. So much for the reliance of heuristics in Posner and Vermeule's theory.

3 CONCLUDING REMARKS

In this first chapter I have expounded my normative assumption that the trade-off model should be rejected in the Union on normative grounds, by appealing to a hermeneutics of the EU constitutional order based on its values in a historical perspective. My analysis is independent from the failures of such *ordre public* determined by short-sighted political action, as discussed in section 2.4.

I argued that challenges to security are quintessentially political, usually embodying controversies over inherently conflicting values. Threats to security trigger heavily political decisions, because the means to address the controversy over values and assets will influence directly the final arrangement and eventually reshape the community. But compressing liberties for the sake of the survival of the nation or, in today's fashion, security, is a typically illiberal approach. Consequently, one cannot use illiberal emergency methods, especially over a long time, to preserve an order based on democracy and fundamental rights, for which the rule of law is the only workable means among the ones devised thus far, as imperfect as it may be. In the words of AG Saugmandsgaard Øe,

> *"The requirement of proportionality strictu sensu implies weighing the advantages resulting from (a) measure in terms of the legitimate objective pursued against the disadvantages it causes in terms of the fundamental rights enshrined in a democratic society. This particular requirement therefore opens a debate about the values that must prevail in a democratic society and, ultimately, about what kind of society we wish to live in."*[287]

[286] Marianne Barland and others, *Report on decision support testing* (SurPRISE Project Deliverable D 7.1, 2014).
[287] *Joined cases C-203/15 and C-698/15 - Opinion of AG Saugmandsgaard Øe*, para 248.

We also risk playing into the hands of terrorists. The strategy of Al Qaeda expounded in the *Idarat at Tawahoush* ((The Management of Savagery, also followed by ISIS), consists in undermining citizens' trust in the ability of governments to deliver security, thus hoping to accelerate a moral, political and social revolution.[288] This would lead to the establishment of what Arendt would have probably labelled a new totalitarian state. Obliterating all that has been built and receding to a Hobbesian conception of *vouloir vivre* would merely serve the terrorists' interests. The ECtHR has put this clearly in *Szabó and Vissy v. Hungary* (referring to *Digital Rights Ireland*):

> *"Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court ...[emphasises] the importance of adequate legislation of sufficient safeguards in the face of the authorities' enhanced technical possibilities to intercept private information."*[289]

This chapter has set the tone for the methodological critique – *viz*. the discussion as to why trading-off security with privacy should be rejected – raising in passing some of the key concepts, 'security and privacy', that I now turn to analyse.

[288] Scott Atran and Nafees Hamid, 'Paris: the War Isis Wants' *The New York Review of Books* (16 November 2015).
[289] Szabó and Vissy v. Hungary, n. 37138/14, CE:ECHR:2016:0112JUD003713814, para 68.

CHAPTER TWO - 'TRADING-OFF PRIVACY RIGHTS FOR SECURITY' IS METHODOLOGICALLY FLAWED

***Abbiamo** la sicurezza,*
*a patto di non **essere** nessuno.*
Eric Fromm[290]

The normative critique I expounded in the previous chapter intended to show why fundamental rights *should not* be traded-off for security in the Union. Here, instead, I focus on the 'methodological critique' anticipated in chapter 1, section 1. It should be noted that the methodological and normative critiques meet at the intersection of the definitions of security and privacy, which are at the same time the object of the methodological critique, and the norm-laden tools necessary to carry out such critique.

My critique has two converging goals. First, I intend to unveil the inconsistency of the factual claims that security and liberty are *de facto* opposed (i.e., because we lie at the frontier of their independent maximisation), and that giving up liberty is the most efficient solution in the face of an emergency. I do so with reference to 'privacy'. By that matter, and second, I address **hypothesis I**, i.e. the inadequacy of the trade-off model as an intellectual device to appraise the relationship between security and fundamental rights.

In section 1 I introduce my methodological critique, which I develop with reference to 'security v. privacy', the object of this thesis. In this chapter I address two out of three challenges featuring the methodological critique, which I apply respectively to security (section 2) and privacy (section 3). As a result of this analysis I propose a reformulation of the relationship between security and privacy that takes into account concrete examples (section 3 and conclusion).

[290] Eric Fromm, *Avere o Essere?* (Mondadori 1977), p. 136.

1 A METHODOLOGICAL CHALLENGE TO 'SECURITY V. PRIVACY'

The methodological critique of Posner and Vermeule's trade-off model, which I developed in chapter 1, consists of three interrelated parts. First, what do these two terms (security and privacy), that are supposedly in opposition, really mean? Second, are security and privacy the only relevant dimensions to be taken into account? And third, would giving up privacy represent the most efficient solution to achieve security, and, if so, why?

The last part will be the focus of chapter four. As a result, hypothesis I (the inadequate explicatory value of the trade-off model) cannot be fully demonstrated here.

As for the second part, I noted in chapter one (section 1) that technology both substantiates what can be done, and how; in this sense, it acts as a modifier. Only theoretically it is possible to look at technology as a value-free tool:[291] once substantiated in an application, it always embodies value-laden choices, as hidden as they may be. Rather than having a separate section on technology, its role will emerge as the analysis of the first question unfolds. I will look into the role of technology as a modifier of our understanding of security (section 2.3) and privacy rights (sections 3.3.1.4 and 3.3.2.3). Reference to concrete examples of technology will be made in chapter 4 and in part two of the thesis.

The bulk of the chapter is thus devoted to the first part, i.e. rebutting the unfortunate foundations of balancing. I do this by expounding the value of the terms and the importance of 'privacy rights' in relation to the *ordre public* of the contemporary EU (chapter 1). This entails three steps: demonstrating the ambiguous meaning of the two terms; re-framing the two terms within the EU *ordre public*; and finally giving legal purchase to the two terms.

Let us start with the first step. Not only it is questionable whether the terms of the debate are comparable, but also the use of those terms themselves is disputable. Rather than representing discrete and monolithic objects, security and privacy are complex concepts. In viewing them this way, I join those commentators who find that the problem in the trade-off model lies in an overlooking[292] or misunderstanding[293] of the meaning and values embodied

[291] See footnote n. 336.
[292] Solove (2011), *Nothing to hide*. Solove (2007), ''I've Got Nothing to Hide''. Julie E. Cohen, 'What Privacy is for' (2013) 126 Harvard Law Review 1094.
[293] Waldron (2010), *Torture, Terrore and Trade-offs*. Huysman (2006).

by security and privacy. Such a misunderstanding can be explained using Solove's[294] pendulum argument. At times of emergency, the importance of the two concepts is re-assessed. Liberties such as privacy are seen as hindering security, and hence their enjoyment should be 'temporarily' compressed. The other side of the coin, epitomized by the war on terror, is that the threat to security is so fundamental as to justify the adoption of any measure, including the limitation of liberties. In this respect, it can be said that the trade-off model finds fertile ground in the securitization of risks or threats,[295] which consists exactly in attributing existential value to a particular threat justifying the adoption of any measure. In other words, there is a trade-off because the value of security swings towards its maximum level, becoming prized above anything else.

The immediate advantage of securitization, namely prioritizing an issue on the political agenda, hinders an appraisal of the ensuing regulatory framework and policies.[296] Likewise, securitization frustrates an open-minded reflection on the diverse factors surrounding security issues, such as the role of technological constraints. Hence, securitization precludes the analysis necessary to prove whether trading security with privacy is the most efficient solution. As a result, security needs to be reappraised in a legally meaningful way.

When considered within the trade-off model (which rests on the securitization of threats), the depth of rights is diluted, in that the reasons why they were originally safeguarded is suddenly overshadowed. The reverse swing of the pendulum takes place here: there is a trade-off because the value of privacy swings towards its minimum level, becoming an obstacle against achieving the most cherished objective. The case for privacy may be worsened by the fact that the right is presented (in policy discourses) as an excuse to cover misdeeds, or as resistance to intrusive practices carried out for security purposes.[297] Hence attention focuses on the (desired) quantum of privacy:[298] since we have or need little privacy, we can sacrifice it. To be sure, Scott McNealy's infamous aphorism as the CEO of Sun Microsystems "you have zero privacy anyway" so "get over it",[299] remains unmatched by politicians. Yet, the mantra that "if you have done nothing wrong, you have nothing to hide",[300] works on the same reductive trail: since the quantum of privacy needed by law-abiding citizens is very

[294] Solove (2011), *Nothing to hide*.
[295] Buzan, Weaver and Wilde (1998).
[296] Huysman (2006).
[297] Solove (2011), *Nothing to hide*; Gloria González Fuster and others, *Discussion Paper on Legal Approaches to Security, Privacy and Personal Data Protection* (PRISMS Project Deliverable D 5.1 2013).
[298] It could be said that securitization transforms privacy into a thin-descriptive concept.
[299] Polly Sprenger, 'Sun on Privacy: 'Get Over It'' Wired (26 January 1999).
[300] Solove (2011), *Nothing to hide*; Solove (2007), ''I've Got Nothing to Hide''.

limited, they should not be worried vis-à-vis the government's attempt to intrude upon it. The same consequence described for security applies here: undervaluing privacy flattens its other dimensions, in this case those concerning its value, and hinders an evaluation of the effects of a regulatory framework and policies limiting it. In order to seriously appraise the concept, we need to restore its full normative meaning.

Hence, both security and privacy lack some meaning, descriptive in the first case, normative in the second. To maintain coherence in the discussion, I tackle each concept separately. In doing so, I also develop the remaining two steps.

Hence, in section two, after having challenged the inflated[301] value of security (section 2.1), I set out to examine its legal value in the Union (section 2.2), where I unveil that it is an expression of the absence of threats codified in offences. Legal descriptive meaning is therefore obtained by substituting 'security' with specific offences.

In section 3 I consider privacy, whose value as a moral[302] and legal entitlement is overlooked (section 3.1). In the Union's legal order, privacy has a double meaning, that of two qualified rights, which must be kept separate: private and family life and the protection of personal data (section 3.2). I then set out to add legal-normative import by recalling privacy's role in protecting "the individual's interest in becoming, being, and remaining a person",[303] i.e. on personhood achieved through intimacy[304] and paving the way to the objective of autonomy so much needed in democracy[305] (section 3.3.). In so doing, I also defend the independence of the right to the protection of personal data.

As a final remark, although contesting the use of security and liberty as terms of reference, let alone their comparability, would be a valid exercise in any democratic society, the specific meaning of their dimensions, once unpacked, changes according to (legal) culture. This is because the range of available responses to threats (and values) are jurisdiction-specific; a

[301] Jeffrey H. Reiman, 'Driving to the Panopticon: Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future (Symposium Paper)' (1995) 11 Santa Clara Computer and High Technology Law Journal 27; Cohen (2013).
[302] Entitlements we believe people should have irrespective of their legal acknowledgment. Reiman (1995).
[303] Jeffrey H. Reiman, 'Privacy, Intimacy and Personhood' in Ferdinand David Schoeman (ed), *Philosophical dimensions of privacy: an anthology* (Cambridge University Press 1984), p. 314.
[304] See, inter alia, Westin (1967). Ferdinand David Schoeman, *Philosophical Dimensions of Privacy: an Anthology* (Cambridge University Press 1984); Julie C. Inness, *Privacy, Intimacy and Isolation* (Oxford Scholarship Online (2003) 1996).
[305] Among others: Cohen (2013); Yves Poullet and Antoinette Rouvroy, 'The Right to Informational Self-determination and the Value of Self-development. Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (2009).

similar claim can be made for rights, at least insofar as their interpretation is concerned. Hence, adding legal-descriptive meaning to security, and legal-normative meaning to privacy, is a contextual exercise, onto which I move now.

2 THE MEANING OF SECURITY IN THE EU LEGAL ORDER

I begin with an analysis of the concept of security (and threats to security) in the literature, intended to show its poor descriptive import (section 2.1). Then, I claim that its malleability is reflected in the EU legal system, where security does not bear any independent legal value, thus requiring a resort to legally more robust terms of reference (section 2.2). In order to add legal-descriptive value to the notion of security, I move on to anchoring the term to appropriate legal descriptive contents in its use within the AFSJ (section 2.3). Security is thus 'reworked' to signify the expression of the absence of threats codified in offences (meaning substantive conduct, i.e. a conduct that constitutes a threat and has been criminalized), and hence any reference to security in a given discussion of the 'trade-off' must be replaced by the specific offence under analysis. I build such reasoning on the example of terrorism in the EU. The final point concerns how offence-related actions are implemented through technology.

2.1 NOTIONS OF SECURITY IN THE LITERATURE

Security is often described in terms of safety,[306] the absence of threats, risks, or fear thereof,[307] and, more recently, 'resilience', i.e. the ability to recover from the concretization of threats;[308] philosophically, it has been associated with legal certainty and predictability (Bentham), or safety and survival (Hobbes)[309] (chapter 1, section 2.1). By trading-off privacy, who earns what kind of security? The answer may not be immediate, as Waldron notices that

[306] Waldron (2010), *Torture, Terrore and Trade-offs*.
[307] Cameron (2000); Huysman (2006).
[308] Regina Berglez and Reinhard Kreissl, *Report on security enhancing options that are not based on surveillance technologies* (SurPRISE Project Deliverable D 3.3, 2013).
[309] Waldron (2010), *Torture, Terrore and Trade-offs*.

such a point is often overlooked.[310] Authors agree on the fact that security is a dynamic and relational term, and the qualifying adjective has a bearing on the question of who earns what kind of security.

The trade-off model often implicitly refers to *national* security, understood as the survival of the state (as opposed to the individual) *vis-à-vis* extreme threats.[311] Maintenance of security acts as a legitimizing factor for the exercise of power.[312] Synonyms derived from the case law of the Strasbourg Court, which has been reluctant to provide a fully-fledged definition,[313] include state security, national safety, and defence of the state (or the realm). But the state could also claim legitimacy by delivering *social* security, as enshrined in article 22 of the Universal Declaration of Human Rights[314] (hereafter UDHR), through welfare programmes.

Moving to a horizontal relationship between states,[315] *international or collective* security concerns the absence of (armed) conflict. Military security refers to a similar concept. The last decade and a half has witnessed the development of *cyber*security, whose meaning is debated, as I expound in the next chapter (section 3).

Many of the elements mentioned above are included and re-elaborated in the all-encompassing concept of *human* security,[316] which develops Roosevelt's idea of freedom from want (relating to the economic and social sphere) and freedom from fear (relating to physical and emotional threats), and which is centred on the individual, rather than the group.

The dialectic between the state and the individual is at the heart of the *right to* security, enshrined in articles 3 UDHR, and 9 ICCPR, which is the heir of *habeas corpus*[317] and embodies the guarantee against arbitrary deprivation of liberty perpetrated by the state. According to the Human Rights Committee (hereafter HRC), security concerns freedom from intentionally inflicted injury to the body and the mind, or bodily and mental integrity,

[310] Ibid.
[311] Ibid.
[312] Cameron (2000).
[313] Ibid; Council of Europe (2015), point 14; Council of Europe (2013). See also the case (declared inadmissible) of Esbester v. the United Kingdom, n. 18601/91, CE:1993:0402DEC001860191.
[314] Universal Declaration of Human Rights (UDHR). General Assembly of the United Nations, Resolution 217, 10 December 1948.
[315] Huysman (2006).
[316] United Nations, Development Programme (UNDP), *Human Develpoment Report* (Oxford University Press, 1994).
[317] Giovanni Pugliese, 'Appunti per una Storia della Protezione dei Diritti Umani' (1989) 43 Rivista trimestrale di diritto e procedura civile 619-659.

irrespective of a state of detention,[318] which includes *foreseeable* threats from governmental as well as private actors. In this respect, the right cannot be seen as justifying the state in taking action for the sake of guaranteeing an abstract meaning of security. Moreover, while the HRC mentions a duty of the state to protect an individual's liberty from abduction or detention by criminals, including terrorists, no such reference is made in relation to a duty to protect an individual's security in relation to terrorism.

It is clear that different notions of security provide different answers to the question 'who earns what kind of security?' and would call for different actions. Waldron's description of security seems to the point: "something we provide for each other by enjoying together the social order of activity and interaction that defines our way of life and by acting in solidarity with one another to ensure that benefits of this system is available to all".[319] Hence, trading-off security with privacy can mean different things depending on the meaning of security envisaged. Security seems a catchall term used to justify any action, and this, as Orrù[320] suggests, may be the best evidence of the fact that this is a (philosophically thin-evaluative) notion with little descriptive power. In the end, it boils down to the way of life, the *vouloir vivre* that we are trying to protect (chapter 1); security may not be the best way of defining that, after all.

2.2 NOTIONS OF SECURITY IN THE TREATIES AND THE CHARTER

Having concluded that the concept of 'security' does not rest on firm ground, the second step consists in appraising whether it acquires greater consistency when inserted in a legally binding text, notably the Treaties and the Charter.

The few instances in which the term 'security' appears alone[321] do not allow for carving out a univocal meaning. In other instances, the term is accompanied by qualifying adjectives

[318] Human Rights Committee, *General Comment n. 35. Article 9 (Liberty and security of person)* (CCPR/C/GC/35, 2014), paras 3 and 9.
[319] Waldron (2010), *Torture, Terrore and Trade-offs*, p. 158.
[320] Elisa Orrù, 'Surveillance, Security and Legitimacy in the European Union' in Elisa Orrù, Maria Grazia Porcedda and Sebastian Volkmann (eds), *Surveillance and control beyond the security v. privacy model* (Nomos Verlag forthcoming).
[321] In article 3.5 TEU (international order), 21 TEU (own security) and 346 (Member States' essential interests to their security).

that enable distinguishing different uses, akin to the ones discussed above. The Treaty refers to 'national' and 'internal security' as a limitation of its competences (4 TEU, 72 and 276 TFEU), to insulate itself from harm (71 TFEU), and to enable Member States' cooperation (73 TFEU) in the context of the AFSJ. As seen in chapter 1 (section 2.4), public security can be a ground for derogating from the four freedoms (36, 45, 52, 65 and 202 TFEU[322]). 'International' security appears in the context of the CFSP (21 TEU) and CSDP (42 TEU), the pursuit of which requires coordination to avoid adverse effects on the internal market (347 TFEU). But the Treaty embodies notions of social security (22, 48, 153, 156 TFEU and Protocols n. 12 and n. 33) eliciting freedom from want. Security is further found in the expressions 'security of energy supply' (art. 194 TFEU), 'security environment' (Protocol n. 10) and accompanied with 'law and order' (art. 4 TEU, 72, 276 and 347 TFEU). The term is a standard feature of the expressions AFSJ, CFSP and CSDP. Finally, the Charter protects the right to liberty and security (art. 6), which has to be understood in the traditional sense of protecting individuals from undue deprivation of liberty.[323]

It can be concluded that the Treaty embodies different conceptions of security.[324] Though this may be a conscious choice, leaving room for political leeway at various levels, security nonetheless lacks descriptive grip. This does not lead necessarily to the conclusion that the term should be discarded altogether, but rather suggests the following preliminary conclusions: the very fact that 'security' is a catchall rhetorical tool hinders an analytical approach to its various uses. A more reliable, and legally sound, substantiation of the term is warranted. The next section tries to add descriptive meaning with reference to the AFSJ (and counterterrorism).

[322] In conjunction with public morality, public health and public policy depending on the article.
[323] Judgment of 16 July 2015 in Lanigan, C-237/15 PPU, EU:C:2015:474; European Union Network of Independent Experts on Fundamental Rights (2006).
[324] Nicholas Grief, 'EU Law and Security' (2007) 32 European Law Review 752-765. González et al. identified six different understandings of security in EU law, namely as in the CFSP, as in the AFSJ, as a limitation of EU primary law, as a ground to restrict free movement, as in NIS and cyber-security and protecting classified information. González Fuster and others (2013).

2.3 THE REFERENCE TO OFFENCES IN THE AFSJ, AND THE HIDDEN ROLE OF TECHNOLOGY

Security expresses the absence of threats, the definition of which depends in turn on the accompanying adjective. In the case of the trade-off, securitizing speech acts depict the threat or security risk as an existential one. An example could be "seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation",[325] typically in the guise of terrorism. For all its emotive charge, terrorism ultimately consists of threatening human conduct. The debate as to whether such conduct should be classified as an act of war, and hence to be dealt with either by *ius ad bello* and *ius in bello*, or alternatively by criminal law, is unresolved, as testified by the failure to develop an internationally recognized definition of terrorism (though the Special Tribunal for Lebanon has made an attempt[326]). Similarly unresolved is the extent to which freedom fighters should represent a special category.[327]

The EU has chosen to treat terrorism as a criminal offense devoid of political meaning. In other words, in the EU terrorism is the result of a wicked conduct and codified as such as an offence in a substantive criminal rule. Such a rule is enshrined in article 1 of the Framework Decision on Terrorism[328] (currently under revision[329]), and consists in the perpetration, or threat to perpetrate, the following acts against a country or an international organisation: "(a) attacks upon a person's life which may cause death; (b) attacks upon the physical integrity of a person; (c) kidnapping or hostage taking; (d) causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss; (e) seizure of aircraft, ships or other means of public or goods transport; (f) manufacture, possession, acquisition, transport, supply or use of weapons, explosives or of nuclear, biological or chemical weapons, as well as research into, and development of, biological and chemical weapons; (g) release of dangerous substances, or causing fires, floods or explosions the effect of which is to endanger human life; (h) interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life."

[325] Article 1 of Framework Decision 2002/475/JHA on Combating Terrorism.
[326] Galli and Weyembergh (2012).
[327] Ibid.
[328] Framework Decision 2008/919/JHA on Combatting Terrorism.
[329] European Commission (2015), *Proposal for a Directive on combating terrorism, COM (2015) 625 final*.

The Framework Decision has been met with criticism, particularly in its revised form adopted in 2008 to embrace the requests, codified in UN Security Council Resolution 1624 (2005), of criminalizing terrorism-related conduct online, even when inchoate (pursuant to article 3 (3), criminalization occurs even in the absence of the actual perpetration of a terrorist offence).[330] What matters for this chapter, however, is to stress that the most feared threat to security, terrorism, is part of criminal law. Consequently, it cannot warrant an indiscriminate war against terrorism, such as has unfortunately been waged recently by France,[331] and, crucially, it can only be substantiated in specific conducts (the precise definitions of which, obviously, matter from a rule of law perspective). In this way descriptive-legal value is added to the term.

Accordingly, 'security v. privacy' becomes 'combating terrorism v. enjoying privacy' or, better, 'combating the "seizure of aircraft, ships or other means of public or goods transport" for the sake of "compelling a Government or international organisation to perform or abstain from performing any act" v. enjoying privacy'. Only by substituting 'security' with the reference to the specific threatened offence it is possible to approach the subject in legal terms.

It should be noted that this is not an apology of EU counterterrorism policies. For the sake of the fight against terrorism, requests to sacrifice liberties, and notably privacy, have been advanced in relation to an ever-expanding array of measures, in accordance with the preventive approach to risks described in chapter 1 (section 2.4), and reinforced after the Paris attacks.[332]

The offences embodied in the Framework Decisions are further addressed by instruments of secondary law which, due to their cross-border dimension in calling for international cooperation, (mostly, but not always) find their legal basis in the Title V TFEU. Terrorism is among those offences, featuring in article 83.2 TFEU on judicial cooperation together with "trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime".

---

[330] Galli and Weyembergh (2012).
[331] 'Hollande Mantient sa Position: "La France est en Guerre"' *Le Monde* (16 November 2015).
[332] See, for instance *Conclusions of the Council of the EU and of the Member States meeting within the Council on Counter-Terrorism, n° 848/15* (Council 2015).

While the identification of offences being combatted is a necessary step for a fully-fledged appraisal of the trade-off model, it is however insufficient. For what does combatting an offence entail? It means adopting measures for the prevention, detection, investigation, and prosecution of such an offence. For offences relating to terrorism, the desired approach is preventative, and relies heavily on intelligence. This is where the trade-off model reveals its inadequacy, because it overlooks a substantively relevant dimension affecting both sides of the balance: technology. Huysman[333] has noted that the securitization discourse has taken over in expert circles, thus overshadowing the importance of technology in deciding what can and cannot be done, especially when the accent is on prevention.[334] In keeping with the example given above, the formulation of the trade-off should thus be corrected as 'the use of method/tool X to combat (prevent) "seizure of aircraft, ships or other means of public or goods transport" v. the enjoyment of privacy'. Suffice to say here that technology is value-laden, particularly with reference to what it is trying to achieve, from its design phase. The topic will be dealt with again in chapter 4.

3 PRIVACY[335]

In this section I wish to draw attention to the inadequate and hasty references to the concept of 'privacy' vis-à-vis security. The expression trading-off 'privacy with security' is problematic in three respects. To begin with, privacy, similarly to security, is a complex notion susceptible to carrying different meanings and embodying different expectations. Relatedly, flattening 'privacy' into a concept devoid of value serves the logical fallacy of the 'nothing to hide' argument. In fact, the descriptive statement that there may already be little privacy, or that one's privacy is worth little (*vis-à-vis* other entitlements) is used to justify the

[333] Huysman (2006).
[334] See the work of projects such as http://irissproject.eu/, http://respectproject.eu/, www.surprise-project.eu, and https://surveille.eui.eu/. On the role of technology in combating crime see Cocq and Galli (2012); Reinhard Kreissl and others, *Exploring the Challenges: Synthesis Report* (SurPRISE Project Deliverable D 3.4 2013); Clayton Northouse, *Protecting what matters. Technology, Security, and Liberty since 9/11* (Computer Ethics Institute, Brookings Institution Press 2006); Levi and Wall (2004).
[335] This section will appear, in a shorter version, in Maria Grazia Porcedda, 'The Recrudescence of 'Security v. Privacy' after the 2015 Terrorist Attacks, and the Value of 'Privacy Rights' in the European Union' in Elisa Orrù, Maria Grazia Porcedda and Sebastian Volkmann (eds), *Surveillance and control beyond the security v. privacy model* (Nomos Verlag forthcoming).

statement of value that there ought not to be too much fuss about privacy.[336] Such a statement of value hides the important role individual and collective privacy plays in a democratic society.[337] Finally, similarly to 'security', the notion of privacy acquires a special significance in the EU. Legally, it may be said it has unclear import, and is substituted by a double reference, that of two qualified rights which must be looked at separately by law and value: private and family life, and protection of personal data.

The discussion, which builds on previous work of mine,[338] develops and integrates existing literature.[339] In order to render legal-normative meaning to privacy, I develop my argument in three steps. First, I unveil the slippery meanings of the term: I discuss the different senses connected to the notion of privacy, and relatedly the fact that, in Europe, two different notions are used to embrace privacy's different aspects (section 3.1). Secondly, I anchor the analysis in the EU legal framework, where privacy embodies two rights (section 3.2). And lastly, since this slippery meaning is connected to degrading the value inherent in the right, I set out to add normative grip with reference to the EU's *ordre public* (section 3.3), following calls for an interdisciplinary approach to rights, particularly in sociology.[340] I experiment with a law and society approach to speculate on the factors that enhanced the emergence of the limbs contained in the legal formulation of the rights (and, contextually, I defend the significance and independence of the right to the protection of personal data). In doing so, I highlight the

[336] In this respect, it could be said that security and privacy are philosophically thick concepts. In philosophy, 'thin' concepts are either descriptive or evaluative/normative, whereas 'thick' concepts are both descriptive and evaluative/normative. During her speech at the conference New Philosophical Perspectives on Surveillance and Control: Beyond the Privacy versus Security Debate (FRIAS, Freiburg, 5-6 November 2015), Prof. Rafaela Hillerbrand noted that drawing evaluative conclusions based on thin descriptive concepts (and vice versa) does not produce a thick concept, but rather expresses a logical fallacy. The trade-off model may transform security and privacy as thin concepts, though in different ways, and lead to several logical fallacies.

[337] Cohen (2013); Solove (2011), *Nothing to hide*; Priscilla Regan, 'Privacy as a Common Good in the Digital World' (2002) 5 Information, Communication & Society 382–405.

[338] Maria Grazia Porcedda, Mathias Vermeulen and Martin Scheinin, *Report on Regulatory Frameworks Concerning Privacy and the Evolution of the Norm of the Right to Privacy*, SurPRISE Project Deliverable 3.2 (European University Institute 2013) <http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE_D3.2_Report-on-regulatory-frameworks-concerning-privacy-for-final-formatting_v094.pdf>.

[339] To mention a few: Reiman (1984), 'Privacy, Intimacy and Personhood'; Schoeman (1984); Inness (1996); Stefano Rodotà, 'Data Protection as a Fundamental Right' in Yves Poullet, Serge Gutwirth, Paul De Hert, Sjaak Nouwt and Cécile de Terwangne (eds), *In Reinventing Data Protection?* (Springer 2009); Poullet and Rouvroy (2009); Solove (2011), *Nothing to hide*; Cohen (2013); González Fuster and others (2013); Orla Lynskey, *The foundations of EU Data Protection Law* (Oxford University Press 2015); Maria Tzanou, 'EU Counter-terrorism Measures and the Question of Fundamental Rights: The Case of Personal Data Protection' (PhD thesis, European University Institute 2012); Lee A. Bygrave, *Data Privacy Law. An International Perspective* (Oxford University Press 2014); Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Erik Claes, Serge Gutwirth and Antony Duff (eds), *Privacy and the criminal law* (Intersentia 2006); Kreissl and others (2013).

[340] Pugliese (1989); Bobbio (1997); Cohen (2013).

role technology has played in shaping, but also in protecting, the two rights. A thorough legal analysis of the two rights will be contained in chapters 6 and 7.

3.1 PRIVACY: ONE ALL-ENCOMPASSING WORD, GLOBALLY

The first step to add normative grip is to show the complexity of 'privacy' irrespective of any jurisdiction. Hence, the purpose of this section is to expound that 'privacy', similarly to 'security', is an umbrella term, and that requests to give up privacy may in fact entail giving up several entitlements. The birth of privacy as a legal concept is typically linked to the famous article written by Warren and Brandeis at the end of the XIX Century for the Harvard Law Review.[341] Quickly labelled as 'the right to be let alone', pursuant to an expression coined by Judge Cooley, privacy was initially subsumed under tort law,[342] not least due to the circumstances that motivated Warren and Brandeis to write their article (discussed *infra*, section 3.3.1.1). Article 12 UDHR gave privacy the seal of a legally acknowledged right. The formulation of article 12 UDHR was almost entirely transcribed into article 17 ICCPR, the first legally binding formulation of the right, which reads

> *1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.*

The Human Rights Committee has avoided providing strict definitions of the dimensions of article 17,[343] an approach followed by other courts on similar matters, as will be discussed more in depth in chapters 4 and 5. According to commentators, privacy includes identity, integrity and intimacy, relating to the body, acts and information, and autonomy of action;[344] family is broadly interpreted and understood as in the state party at stake;[345] home is the place

[341] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1980) 4 Harvard Law Review.
[342] Articulated by William Prosser, 'Privacy' (1960) 48 California law review 383-423. Privacy was initially addressed under tort law also in Germany: Spiros Simitis, 'Privacy - An Endless Debate' (2010) 98 California law review.
[343] Human Rights Committee (CCPR), *General Comment n. 16. Article 17 (The right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation)* (1988).
[344] Manfred Nowak, 'Chapter on Article 17 ' in Manfred Nowak and Felix Ermacora (eds), UN Covenant on Civil and Political Rights, CCPR Commentary (N.P. Engel 2005 (2nd edition)).
[345] Human Rights Committee (CCPR) (1988).

where one resides or works;[346] correspondence extends beyond letters. Honour and reputation are not defined, but are still protected from attack, e.g. as deriving from having one's name and full contact details published on the UN Security Council's terrorist list.[347] Oftentimes 'the right to privacy' is used as a synecdoche to refer to all dimensions of article 17 ICCPR.[348]

At the times when the ICCPR was adopted, the consequences of applied informatics, particularly in relation to private and public uses of databases, triggered several scandals[349] that fuelled renewed policy attention on privacy. Alan Westin was the author of another popular definition of privacy, i.e. "the control over personal information"[350] which could be processed in such databanks (although, in his treatise, he seems to broaden the scope beyond that definition[351]). Westin's work was at the basis[352] of the development of the 'fair information principles',[353] which oversee the functioning of 'information privacy'. Such understanding of privacy was given legal, if non-binding, substance[354] by the OECD 1980 Privacy Guidelines (revised in 2013[355]), which lay down rules allowing and limiting the control over information relating to any identified or identifiable individual (personal data).

Westin's work paved the way to a stream of studies that still thrives today (this thesis being a manifest example!); ever since, scholars competed to provide the ultimate definition of privacy.[356] Some authors searched for the dimensions of privacy worthy of protection.

---

[346] Ibid; Nowak (2005 (2nd edition)); John Blair, *The International Covenant on Civil and Political Rights and its (First) Optional Protocol. A Short Commentary Based on Views, General Comments and Concluding Observations by the Human Rights Committee* (Peter Lang 2005).
[347] Sayadi and Vinck v. Belgium, Communication n. 1472/2006, CCPR/C/94/D/1472/2006.
[348] To this effect, Scheinin (2009), *Report on Human Rights and Fundamental Freedoms while Countering Terrorism*.
[349] Stefano Rodotà, *Elaboratori Elettronici e Controllo Sociale* (Mulino 1973); Abraham L. Newman, *Protectors of Privacy. Regulating Personal Data in the Global Economy* (Cornell University Press 2008).
[350] Westin (1967).
[351] His second definition of privacy, in fact, encompasses the dimensions partly recognized by the law: "viewed *in terms of the relation of the individual to social participation*, privacy is the *voluntary and temporary withdrawal* of a person from the general society through physical or psychological means, either in a state of solitude, or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve" ibid, p. 5.
[352] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right in Europe* (Springer 2014).
[353] Robert Gellman, 'Fair Information Practices: A Basic History (Version 1.89)' (2012). Constantly updated at: <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>.
[354] González Fuster (2014).
[355] Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Organization for the Economic Cooperation and Development, C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79.
[356] For a non-exhaustive list of attempts: Schoeman (1984); Simitis (2010); Colin Bennett and others, 'Special Debate Section Discussing Bennett's Essay 'In Defense of Privacy'' (2011) 8 Surveillance & Society 485-516; Rodotà (2009), 'Data Protection as a Fundamental Right'.

Westin[357] found solitude, intimacy, anonymity and reserve; Fried[358] identified privacy as key for respect, love, friendship and trust; Clarke[359] isolated the privacy of the person, of behaviour, of personal communications and of personal data; Finn et al. [360] added to Clarke's list privacy of thoughts and feelings, of action, of image, of location and space, and of association (including group privacy). Solove [361] preferred taking inspiration from Wittgenstein's concept of family resemblances, while Nissenbaum[362] suggested concentrating on context, and Regan[363] to look at privacy as a common good. The list could continue.

I do not privilege any single author's definition, as I take the view that privacy encompasses all abovementioned dimensions, including the goal of protecting personal data, which makes it, as González Fuster notes,[364] inherently ambiguous. In this respect, I agree with Solove[365] in that privacy is an umbrella term[366] and that, as I detail later on, it is fundamentally dynamic,[367] because I ideally belong in a group of authors[368] that consider privacy instrumental to the development of identity/personhood based on intimacy and leading to autonomy. What is fundamental for the development of identity and personhood cannot be defined once and for all. Nonetheless, I concur with Bennett that, for all the scholarly criticism, the term has too much intellectual and political[369] grip to be set aside.[370] As a result, in the EU legal order it may be more correct to talk about 'privacy rights', taking into account the caveats that I formulate in the next section.

---

[357] Westin (1967).
[358] Charles Fried, 'Privacy (a moral analysis)' in Ferdinand David Schoeman (ed), *Philosophical dimensions of privacy: an anthology* (Cambridge University Press 1984).
[359] Roger Clarke, 'What's 'Privacy'? Version of 7 August 2006' (Workshop at the Australian Law Reform Commission).
[360] Rachel L. Finn, David Wright, and Michael Friedewald, 'Seven Types of Privacy', in Ronald Leenes, Serge Gutwirth, Paul De Hert, and Yves Poullet (eds.), *European Data Protection: Coming of Age* (Dordrecht: Springer, 2013)
[361] Daniel Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy', San Diego Law Review, 44 (2007).
[362] Helen Nissenbaum, 'From Preemption to Circumvention: if Technology Regulates, Why Do we Need Regulation (and viceversa)?' (2011) 26 Berkeley Technology Law Journal 1367-1386.
[363] Regan (2002).
[364] González Fuster (2014).
[365] Solove (2007), ''I've Got Nothing to Hide''.
[366] Though according to Andrade, the role of umbrella term should be covered by 'personal identity', which is unduly superimposed to 'privacy' and 'data protection'. Norberto Andrade, 'The Right to Personal Identity in the Information Age. A Reappraisal of a Lost Right' (PhD thesis, European University Institute 2011).
[367] Cohen (2013), p. 1906.
[368] Like Westin, Reiman, Gavison (Ruth Gavison, 'Privacy and the Limits of Law' in Ferdinand David Schoeman (ed), *Philosophical dimensions of privacy: an anthology* (Cambridge University Press 1984)), Inness and Cohen.
[369] Colin Bennett and Charles Raab, *The Governance of Privacy. Policy Instruments in a Global Perspective* (The MIT Press 2006).
[370] Bennett and others (2011).

By means of an interim conclusion, from the vantage point of this discussion, the statement "trading-off security with privacy" should appear increasingly emptier. Building on the example used earlier, the statement should be reformulated accordingly, e.g. "using the method/tool X to combat (prevent) the 'seizure of aircraft, ships or other means of public or goods transport' at the expense of X as 'privacy of location and space'.

3.2 'PRIVACY RIGHTS' IN THE EUROPEAN UNION

The second operation needed to add normative grip to 'privacy' is to anchor it in the EU legal framework, where, despite its appeal, the concept bears uncertain legal significance, as it embodies (at least[371]) two rights which should be looked at separately.

To be sure, the CJEU has recalled that "EU law must be interpreted in the light of the relevant rules of international law, since international law is part of the European Union legal order and is binding on the institutions",[372] and therefore the formulation in article 17 ICCPR cannot be, and has not been,[373] ignored. However, the EU is not party to the ICCPR, and even if it were, the parts thereof which are not customary in nature,[374] (or peremptory) would not supersede written primary law such as the Charter[375] but rather, as the CJEU has long held, "supply guidelines to which regard should be had".[376] The same argument can be made in relation to the Council of Europe's Convention 108[377] (further discussed in chapter 7).

As the seminal work carried out by González Fuster[378] demonstrates, no mention is made of 'privacy' in primary law. As for secondary law, privacy is inconsistently referred to, alongside the expressions 'private life' and 'protection of personal data';[379] the same can be said for judgments interpreting such secondary law (discussed in chapters 6 and 7).

[371] The right to personality (see footnote n. 366) and to identity is advanced by Andrade (2011).
[372] Judgment of 16 October 2012 in Hungary v. Slovakia, C-364/10, EU:C:2012:630, para 44.
[373] European Parliament (2014), *Inquiry on the Electronic Mass Surveillance of EU Citizens*.
[374] Marise Cremona, *External Relations of the EU and the Member States: Competence, Mixed agreements, International Responsibility, and Effects of International Law* (European University Institute Working Paper LAW 2006/22, 2006).
[375] Rosas and Armati (2010).
[376] Judgment of 13 July 1989 in Wachauf v. Bundesamt Für Ernährung Und Forstwirtschaft, C-5/88, EU:C:1989:321, para 17.
[377] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS n. 108, 28 January 1981.
[378] González Fuster (2014).
[379] Ibid.

Translations of applicable law betray an even more inconsistent use of terms. The General Data Protection Regulation[380] (hereafter GDPR) replacing Directive 95/46/EC, currently overseeing the protection of "the right to privacy with respect to the processing of personal data" (with language taken directly from Convention 108[381]), contains no references to privacy as such.

In the EU legal order, the various dimensions encompassed by 'privacy' are divided between two qualified rights, both enshrined in the Charter.

Article 7 on respect for private and family life derives from article 8 ECHR (which contains no reference to 'privacy'), which in turn is rooted in article 12 UDHR.[382] The questions of the overlap of article 7 of the Charter with article 8 ECHR (something which González Fuster[383] is critical of), and of what constitutes its essence, will be dealt with in chapter 7. Suffice to say here that both rights give legal protection to those elements of privacy concerning private life, home, relationships and communications.

Article 8 on the protection of personal data embodies those elements of privacy that pertain to personal information and the free flow thereof, which are currently dealt with by Directive 95/46/EC and 2002/58/EC,[384] but without the connection to the internal market. The right, now enshrined in article 16 TFEU and 39 TEU, seems to be a disputed child,[385] with many potential parents including both former article 286 EC, and Convention 108 of the Council of Europe (further discussed in chapter 7, section 1).

González Fuster[386] and Linskey[387] rightly note that scholars who wish to treat the two rights separately have to justify the independence of personal data protection from article 7 of

[380] Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1.
[381] Moreover, the revised version of Convention 108, under discussion at the time of writing, seems to substantially reduce references to 'privacy'. Council of Europe, *Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data* (2016).
[382] Council of Europe, European Commission of Human Rights, 'Preparatory work on Article 8 of the European Convention on Human Rights' < http://www.echr.coe.int/library/COLFRTravauxprep.html>.
[383] González Fuster (2014).
[384] 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, OJ L 201 (E-privacy Directive).
[385] European Parliament, Council and Commission (2002), Explanations to the Charter.
[386] González Fuster (2014).
[387] Lynskey (2015).

the Charter.[388] To an extent, my own analysis will not differ (*infra*, section 3.3.2). Part of the problem in dealing with the matter is that, before the Charter became legally binding, the CJEU could only rely on article 8 ECHR, which encompasses not only the traditional and the informational dimensions of privacy, but also elements, such as environmental protection (discussed in chapter 6), which are not associated with privacy at all. A second problem lies in the unfortunate formulation of Directive 95/46/EC (the right to privacy with respect to the processing of personal data), which has understandably been replicated in judgments on the subject matter. Very few judgments, thus far, concern article 8 taken alone (as discussed in detail in chapter 7), though the recent opinion on *Tele2 Sverige*, in which AG Saugmandsgaard Øe in an *obiter dictum* argued that article 8 of the Charter does not correspond to any rights guaranteed by the ECHR,[389] may change what Tzanou has rightly called the "data protection paradox".[390]

From the perspective of black letter law, the fact that two rights exist, and that personal data protection is further enshrined in both Treaties, should be a sufficient reason to accept the legitimacy of both rights (and the reference to personal data protection as fundamental[391]). Furthermore, it may be useful to recall that, in the European Union legal order, personal data protection may have had more prominence than the respect for private life, due to the former's internal market dimension, particularly in enabling the free flow of personal data.[392] Although it was not a fundamental right, in *Fisher* the Court said that the principles enshrined in Directive 95/46/EC transposed into EC law general principles which already existed at member states level.[393] On the other hand, while respect for private and family life was a right common to the constitutional traditions of the Member States, and seen as being part of the

[388] Tzanou (2012) argues convincigly that even authors who distinguish the two privacy rights end up explaining the protection of personal data by means of private life, or even argue for a subsidiary position. The former is the case of De Hert and Gutwirth (2006). The latter is the case of Poullet and Rouvroy (2009).
[389] *Joined cases C-203/15 and C-698/15 - Opinion of AG Saugmandsgaard Øe*, para 79.
[390] Tzanou (2012), p. 353. Such paradox stands in the way of the autonomous character of personal data protection. Tzanou argues that the right to personal data protection will become fundamental when two criteria will be satisfied: the right will be able to mandate and prohibit, thanks to the identification of essential cores that cannot be overridden, and must be balanced against opposing principles autonomously (instead of reliance on privacy). I will come back to both points in chapter 7.
[391] González Fuster (2014).
[392] However, Poullet and Rouvroy (2009) argue that this may have been a subsidiary intention from the start For a discussion of the double nature of Directive 95/46/EC and the implications for its legal basis, see Lynskey (2015).
[393] Judgment of 14 September 2000 in Fisher, Case C-369/98, EU:C:2000:443, para 34.

general principles of EU law as early as in the *National Panasonic* case,[394] the right was only relevant in the context of restrictions on the freedom of movement and family reunification.[395]

Both González Fuster[396] and Cremona note the instrumental role played by both rights in the pursuit of the four freedoms. While personal data protection was a limitation against, but also a protection to enable, the free flow of data and the services relying on them, the right to family life went in the direction of supporting freedom of movement. However, the Lisbon Treaty marks the end of the instrumental character of the two rights, which acquire a life of their own. As the EU has embraced new competences in the criminal area, viz. of providing an area of security (articles 3 and 21 TEU), both rights have acquired full, and possibly equal, weight. The potential of greater interference with personal autonomy means that the importance of respecting private and family life transcends the field of freedom of movement. Likewise, protecting personal data is more important *vis-à-vis* intelligence-led policing and profiling (and attacks from the private sector[397]).

This point leads to the final step for reattributing depth to both rights, namely underlining their full value in a democratic society *vis-à-vis* security (see chapter 1). In discussing these points, I will also show the added value of personal data protection.

As an interim conclusion, and in keeping with the example in section 3.1 above, the empty expression 'trading-off security with privacy' could become 'using the method/tool X to combat (prevent) the "seizure of aircraft, ships or other means of public or goods transport" at the expense of the fundamental right to personal data protection'.

3.3 EXPLAINING THE VALUE OF THE TWO 'PRIVACY RIGHTS' IN THE EU

After having legally situated 'privacy', as a final step to challenging the reductive approach to privacy in the trade-off model, I elaborate the normative value of privacy as understood in the EU. In other words, here I discuss what 'privacy rights' are protecting, and

[394] Judgment of 26 June 1980 in National Panasonic v. Commission, C-136/79, EU:C:1980:169, para 17, discussed in Juliane Kokott and Christoph Sobotta, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222-228.
[395] For a discussion of some relevant cases, see chapter 6.
[396] González Fuster (2014).
[397] In this respect, see Cohen (2013).

why it matters in contemporary European democratic society (*vis-à-vis* pressing requests to give it up). To this effect, I follow a law and society approach, and particularly the idea of Bobbio[398] and Pugliese,[399] whereby the importance of any right can only be understood in the light of the social circumstances determining its appearance.[400] Like all other liberties, the two privacy rights were effected by the emergence of new needs resulting from societal, cultural and technological developments.

While implicit in the legal works relating to 'privacy' in the EU, such references are not explored in such works,[401] to the detriment of the understanding of the value of both rights (particularly pronounced with reference to the protection of personal data). I intend to fill the gap to confer importance to privacy again, with a view to demonstrate its valuable relation with the EU *ordre public*.

By looking into those original needs it also becomes possible to embrace without risk of contradiction the connections between the right to private life and personal data protection. Indeed, acknowledging that personal data protection is independent from the right to private life does not exclude an area of overlap (unsurprising *per se* as interdependence is part of the doctrine of human rights). Understanding this area of overlap may also help to explain why the international notion of privacy has come to embrace the goal of personal data protection. Both rights, in fact, are instrumental in fostering personhood, one's unique identity,[402] protected as an expression of dignity, and enabling autonomy as the two rights emerged out of modernity.

I start with the right to private life, and then look into the protection of personal data.

---

[398] Bobbio (1997).
[399] Pugliese (1989).
[400] For a discussion of the deep ties between sociology and human rights, see Brunsma, Iyall Smith and Gran (2013). In the same vein, I agree with Cohen's appeal to look into other disciplines to explain the value of privacy, or rediscover such an interdisciplinary approach, which was visible in early but often-neglected work.
[401] *Inter alia* González Fuster and others (2013); Lynskey (2015).
[402] Instead, for Andrade (2011), privacy can be at odds with identity, because they express two different elements of a broader right to personality. The protection of personal data, which is a procedural right, should be subsumed under a right to identity (distinct from the right to privacy). While the distinction between personality and identity may add an interesting analytical layer, I believe that Andrade's analysis could have led to different conclusions if it had been based on a deeper parsing of the legal and moral conceptual elements of privacy rights. After a deeper reading, in fact, privacy rights prove capable of protecting the possibility of change and of multiple identities.

3.3.1 GIVING NORMATIVE DEPTH TO THE RIGHT TO PRIVATE AND FAMILY LIFE (ART. 7)

Article 7 of the Charter reads: "Everyone has the right to respect for his or her private and family life, home and communications". In the intention of the European legislator (article 52.3 of the Charter), Article 7 derives from and corresponds to article 8 ECHR. The latter is rooted in article 12 of the UDHR, but the drafters of article 8 ECHR chose the English expression 'private life' instead of 'privacy' as the English translation of the French *vie privée* (adding to the babel of formulations pointed at by González Fuster). Unfortunately the *travaux préparatoires* of article 12 UDHR contain scant details of the discussions leading to the adoption of the right. Similarly, the drafters of article 8 ECHR left to future generations limited cues for the rationale for enshrining the right in the Convention. Perhaps this could relate to the lack of substantial philosophical debates on privacy reported by Schoeman that continued until the 1960s. A law and society approach is in this case inevitable, in the attempt to trace back the roots of the right in the near past and relate it to the enlightening, yet constantly evolving interpretations provided, for instance, on article 8 ECHR by the ECtHR. I implement a law and society approach by reflecting on each of the four limbs contained in the legal formulation of the right. I begin with the one closest to 'privacy', private life, the discussion of which also lays the foundations for the approach to the other three limbs, in the sense that I analyse the remaining three limbs in the light of the outcome of the discussion concerning private life.

3.3.1.1 The right's first limb: private life

The acknowledgment of the existence of private life predates the appearance of the right, and can be traced back to the Greek polis, so that it would seem tempting to discuss it by contrast with its antonym 'public'. Following this temptation to reflect on the model of the Greek polis would lead down a dead-end, as Arendt[403] brilliantly expounded. In the ancient Greek civilization, the private coincided with the household, which was at once necessary for men to be free and take part as peers in the public affairs of the city, but also despised as a domain of deprivation from the most quintessentially human achievement of excellence

[403] Arendt (1998), *The Human Condition*.

through speech.[404] Public life, where few enjoyed equality and liberty, could only be practised by those who were relieved from the need to earn their living, something enabled by the (productive) household. The household was in turn the seat of inequality, to maintain which the male leader was entitled to use violence against family members, slaves and employees alike.[405] The household carried with it a sense of deprivation, of withdrawal from the public view, and not partaking in a common life.[406]

This is not what Warren and Brandeis referred to in their article. The authors described privacy as an *emerging* societal, moral and philosophical need in search for legal protection, "a right to personality" or identity, namely the expression of one's life, such as emotions, sentiments, facts of life, happenings, actions, sexual life and relationships with others (implicitly unobserved). The authors believe protecting private life as personality or identity connected to intimacy to be a young need. The point is not that personality or intimacy had never existed before, but that, as Westin[407] noted, it is precisely when these features are both enhanced and threatened – whether because they become matter of public enquiry (Warren and Brandeis), policy (Arendt) or intrusion (Westin) – that they become cherished values requiring legal protection, and enter the realm of freedom. Private life lost its meaning of deprivation in concomitance with the "enrichment of the private sphere through modern individualism",[408] underpinned by the elevation of intimacy to a value.

I believe a succinct account of the social circumstances effecting such changes is necessary to appraise the extent to which the values undergirded by private life matter in today's society. To do so, I adopt the views of Charles Taylor[409] and Hannah Arendt[410] concerning late modernity, and Westin's (and Arendt's) early work on intimacy that laid the basis for later discussions.[411] Such account[412] entails four moves recalling, on the one hand, the factors that enhanced the surfacing of a given dimension of private life [1], and that challenged them

[404] According to Arendt, Aristotle's adage 'man is by nature political, that is social', is the result of a mistranslation. 'Social', the need of company, was a concept produced by the Romans. For Arendt, such wrong reading is supported by the fact that today's society is organized as an enormous family primarily concerned with production and survival.
[405] Unfortunately the home can still be the theatre of unequal relationships and violence toward women and children, a feature that has led scholars to identify 'privacy' as the excuse for patriarchal domination; Schoeman (1984). However, this may result from conflating 'privacy' with 'secrecy', i.e. forbidding disclosure because of a superior cause, as discussed by Westin (1967).
[406] Arendt (1998), *The Human Condition*.
[407] Westin (1967).
[408] Arendt (1998), *The Human Condition*.
[409] Taylor (1989); Charles Taylor, *The Ethics of Authenticity* (Harvard University Press 1992).
[410] Arendt (1960), 'Freedom and Politics'; Arendt (1998), *The Human Condition*.
[411] *Inter alia* Schoeman (1984); Inness (1996); Cohen (2013).
[412] For a different path leading to similar conclusions situating change in the XIX Century, see Andrade (2011).

[2]; and on the other hand, the mechanism that favoured a legal approach to the concept [3] and the political occurrences that subsequently spurred its recognition as a right [4].

I begin with the enhancing factors [1]. With the passage to modernity, identity stopped being attached to the role inherited at birth, and the former was no longer implicitly recognized. Detaching one's identity from one's social role was effected by the idea of authenticity, i.e. of one's originality. This, according to Taylor, found its roots in the idea that the concepts of right or wrong were anchored in human feelings, in "a voice within,"[413] which is to be listened to if one wants to live a full life. Such an idea, which at the beginning was conceived of as a way to connect to God, lost its religious connotations and came to be associated with intimacy enjoyed in private, whose first advocate was Rousseau.[414] To be sure, intimacy had always existed, and according to Westin[415] it is a quintessentially animal need used in a dialectic manner with sociality. Intimacy is a distance-setting mechanism (within the same species) to reproduce, breed, play and learn, whereas sociality is interpreted as a desire for stimulation by fellows. Patterns of privacy and sociality at the levels of individual, household and community are expressed in different forms in all cultures of the world. Westin refers widely to anthropological work, showing how different devices (Tuaregs' veils, humour, backslapping, fans, or sunglasses) perform the function of distance-setting, the symbolic realization of privacy and withdrawal from society. Reserve, as well as the existence of intimacy, serve the double function of allowing the development of one's personality by making sense of the different roles played by the individual in a community[416] and the safeguarding of one's social status. Taylor notes that the notion of authenticity was fully developed by the father or Romanticism, Johann Herder, according to whom every human being is intrinsically different and original, and has to be true to herself, i.e. live her

[413] Taylor (1992), *The Ethics of Authenticity*, p. 26.
[414] Arendt (1998), *The Human Condition*.
[415] Westin (1967).
[416] Robert F. Murphy, 'Social Distance and the Veil' (1964) 66 American Anthropologist 1257-1274. The point has been then taken in the contributions developed by Schoeman, where for instance Jeffrey H. Reiman argues: "the relationship between privacy and personhood is a twofold one. First, the social ritual of privacy seems an essential ingredient in the process by which 'persons' are created out of pre-personal infants. It conveys to the developing child the recognition that his body to which he is uniquely 'connected' is a body over which he has some exclusive moral rights. Secondly, the social ritual of privacy confirms, and demonstrates respect for, the personhood of already developed persons." He refers to both as "conferring title to one's existence" and further claims "to the extent that we believe that the creation of 'selves' or 'persons' is an ongoing social process…the two dimensions become one: privacy is a condition of the original and continuing creation of 'selves' and 'persons'." Reiman (1984), 'Privacy, Intimacy and Personhood', p. 310.

life her way, as a goal in life, against an instrumental approach to one's life and the levelling demands of the community.[417] This leads to the second move.

Indeed, as mentioned above, while modernity enabled the liberation of the self, the appearance of the nation state, society, and technology threatened reserve and intimacy [2]. Major organizational changes begetting the nation state unleashed the need to intrude into the private sphere in a more extensive way,[418] aided by the evolution of public and private bureaucratic practices notably explained in the work of Weber. Similarly, society emerged when economic activities previously confined in the household became a source of concern for the public realm. Hence, the household – the social – was elevated to the public.[419] In other words, the social realm infused and occupied the space of politics, thus suffocating both politics and private life, and placing levelling demands of conformism. This both threated and spurred intimacy as the antidote against such demands of conformity.

In this respect, Warren and Brandeis' idea of 'being let alone' could be one extreme of the spectrum, coinciding with the choice of excluding any 'significant others' from one's life.[420] As for the emergent consequences of technological progress, that is, in my view, what spurred Warren and Brandeis' contribution.[421] The article contains references to the improvement of long-distance photography and the proliferation of sensational periodicals[422] (the development of the press stemming from the organizational changes above). Warren and Brandeis were writing to protest against the increasing intrusion of the press suffered by Warren into his family affairs, due to the fact that he had entered a politically powerful family by means of marriage. As documented by Gajda,[423] Warren had married Mabel Bayard, a US Senator's daughter. However, differently from the classic account of the origins of the famous essay

[417] Another interesting perspective is that of psychoanalysis, which highlights the importance of the process of differentiation of the individual from the community. See Carl Gustav Jung, *Tipi Psicologici* (Bollati Bornighieri 2011 (fifth edition)); Fromm (1977).
[418] Westin (1967).
[419] Arendt (1998), *The Human Condition*.
[420] But Taylor acknowledged that even the hermit and the solitary artist are engaged in a dialogue with, respectively, God and the future public who will admire the artist's works. Taylor (1992), The Ethics of Authenticity.
[421] And, more in general, the development of identity: Andrade (2011) rightly points out that our description of the evolution of mankind, from Paleolithic to the Information Age, is marked by different stages of technological development.
[422] E.g. "If you may not reproduce a woman's face photographically without her consent, how much less should be tolerated the reproduction of her face, her form, and her actions, by graphic descriptions colored to suit a gross and depraved imagination." Warren and Brandeis (1890).
[423] Amy Gajda, *What if Samuel D. Warren Hadn't Married a Senator's Daughter?: Uncovering the Press Coverage That Led to the Right to Privacy* (Illinois Public Law and Legal Theory Research Papers Series, Research Paper No 07-06, 2007).

given by Prosser,[424] it was neither Warren, nor his wedding, who was the immediate object of attention, but rather his wife and father-in-law, who became himself the focus of gossip columns when he married a lady twenty years younger. From 1882 until 1890, detailed and variously intrusive accounts of the Warren-Bayard family life featured or were mentioned 60 times, often in gossip columns or front page, by the most circulated newspapers, and the 'Right to Privacy' had no practical effect over media attention, including the coverage of Warren's own death twenty years later.[425]

Yet, these developments were not sufficient for the newly discovered values to become legally relevant. Another change was needed: the redistribution of the positive effects of modern individualism thanks to the *telos* of equality of recognition spurred by dignity [3]. Taylor recounts that dignity was the product of modernity linked with the evolving sources of legitimation of the polity and substituting honour. Honour, automatically recognized at birth to few, was previously the basis of pre-determined, social hierarchies ruled by natural law, whereby life was respected in abidance of a superior law. The new social contract that paved the way to democracy hinged on the idea of universal, natural (subjective) rights, whereby life is respected because of the intrinsic value of human beings.[426] Such equal value carried recognition– the social policy of equal recognition, through procedural justice or fairness – and "is now universally acknowledged in one form or another",[427] to the point that its denial can be perceived of as discriminatory. Dignity, the sense of self-worth, is a cornerstone of contemporary legal and political systems: it calls for respect which is accorded to all, and what commands respect is the very fact of being a human being. Respect has also an active meaning, in terms of subjective rights, of freedom and self-control.[428] Indeed, the combined effect of respect for dignity and uniqueness paved the way to the value of autonomy, which stems from what, according to Taylor, seems to be the strongest moral concerns of our time: the respect for life, integrity, and well-being of human beings, which grew from Locke through to Romanticism. "To talk of universal…rights is to connect respect for human life and integrity with the notion of autonomy. It is to conceive people as active co-operators in establishing and ensuring the respect that is due them. This…goes along with…the conception of what it is to respect someone. Autonomy is now central to this…For us

[424] Prosser (1960).
[425] Gajda (2007).
[426] Taylor (1989), *Sources of the Self*.
[427] Taylor (1992), *The Ethics of Authenticity*, p. 49.
[428] Taylor (1989), *Sources of the Self*; Reiman (1984), 'Privacy, Intimacy and Personhood'.

respecting personality involves as a crucial feature respecting the person's moral autonomy".[429]

This leads to the final and decisive move [4]. Fascist and totalitarian regimes demonstrated the dangerous consequences of crushing reserve, intimacy and autonomy, and eased the transition of 'privacy' from a legal category to a fundamental right, from privilege of the élite to a human right. The ideologies supporting fascist and totalitarian regimes aimed at regimenting individuals, in pursuit of a corporatist society where the single is a function of the total.[430] Autonomy, understood as non-conforming action,[431] is instead seen as quintessential to the continuity of democracy. This is the value of private life implicit in the right, and defended by the courts. In *Pretty v. UK*, the ECtHR said "the notion of personal autonomy is an important principle underlying the interpretation of its guarantees".[432] The import of this for our EU democratic society is recalled in section 3.3.3.

3.3.1.2 The right's second limb: family life

Before continuing, I must recall that I revise the value of family life, like the remaining limbs of article 7 of the Charter, in relation to my main argument, i.e. that they are instrumental to personhood, identity and autonomy as the quintessential function of the right, and not to the wider concept of the creation of family, which forms the object of different rights.[433] As a result of such restricted focus, the application of the four-step methodology is necessarily less extended.

Privacy is neither absolute, nor is it exhausted by intimacy. On the one hand, intimacy and reserve enjoyed in private enable us to maintain consistency among the roles played in the

[429] Taylor (1989), *Sources of the Self*, p. 12.
[430] Bobbio (1997).
[431] Arendt (1998), *The Human Condition*.
[432] Pretty v. the United Kingdom, n. 2346/02, CE:ECHR:2002:0429JUD00234602 (tentative), para 61.
[433] Art. 9 (right to marry and to found a family), and art. 24 (rights of the child). How the creation of a family can be encouraged or hindered by social factors is beyond the scope of this work. For a treatise in the American context: Angela J. Hattery and Earl Smith, 'Family' in David L. Brunsma, Keri Iyall Smith and Brian Gran (eds), *The Handbook of Sociology and Human Rights* (Paradigm Publishers, Routledge 2013). Moreover, the debate of how socio-economic factors, including gender, impacted on family types, marriage patterns, and family formation is heated. David I. Kertzer, 'Household History and Sociological Theory' (1991) 17 Annual Review of Sociology 155; Paul Puschmann and Arne Solli, 'Household and Family during Urbanization and Industrialization: Efforts to Shed New Light on an Old Debate' (2014) 19 The History of the Family 1.

face of change, giving sense to one's biography.[434] On the other hand, Westin[435] reminds us how such mechanisms are in dialogue with the need for sociality (and even societal surveillance as a mechanism to enforce norms). One's identity results in particular from the interaction between the mechanism of identification (the sense of belonging to a group) and individuation (defining oneself against the external world and those that do not form part of our group). The development of one's identity could be said to concretize in being able to answer the question "who am I?".[436] Identity is defined through dialogue, by using "human languages of expression"[437] to interact with 'significant others', throughout one's lifetime. Significant others try to recognize a certain identity in us, and it is in dialogue with such encounters that we define ourselves. Such dialogue starts early in life, through different stages of socialization, the first of which takes place in the family.

Family is in fact another crucial component of the private realm. Family is patently the most basic human formation, or community, in which people find themselves and to which they cling for necessity and survival.

Similarly to private life, family life has lost its privative connotation in concomitance with two cultural changes of utmost relevance today. Here I highlight the enhancing and limiting factors that led to the legal significance of family life.

First, Taylor[438] recalls that one of the most fundamental interactions for identity is that of love. The increasing possibility to choose freely one's partners, which places love at the heart of the family, makes family life instrumental to the development of identity. Second, the Reformation made 'ordinary life' more valuable than previous modes of living. Accordingly, the good life was identified with everyday life, spent in the family and in one's productive activity, in worship of God[439] or, from the 19th century, focussing on enjoying the small, charming things.[440]

In parallel to private life, fascist and totalitarian regimes also tried crushing family life, which should have either mirrored the organization of the regime, or be annihilated; the prohibition of interracial marriages, as well as using children to report non-conforming

[434] Arnaldo Bagnasco, Marzio Barbagli and Alessandro Cavalli, *Sociologia, Cultura e Società. I concetti di base* (Il Mulino 2001), p. 167.
[435] Westin (1967).
[436] Bagnasco, Barbagli and Cavalli (2001), p. 167.
[437] Taylor (1992), *The Ethics of Authenticity*, p. 33.
[438] Taylor (1989), *Sources of the Self*.
[439] Ibid.
[440] Arendt (1998), *The Human Condition*.

political activities of parents, showed the risks of annihilating the protection afforded to the family. Indeed, such experiences were among the reasons used in support of the adoption of article 8 ECHR as described in the *travaux préparatoires*.[441]

The importance of enjoying life with one's partner and spent with the family is confirmed by secondary legislation on family reunification recognized, for instance, in relation to citizens taking advantage of the freedom of movement pursuant to article 21 TFEU.[442] In *Metock,* the ECJ referred to "normal family life", which is in line with (mostly) consistent case law on the matter.[443] Glendon notes how family life, self-determination and individual privacy contributed over time to deregulation, stressing her concern that the retreat of law can foment an undue prevalence of private power relations; "where general ideas about the conduct of family life are expressed in the law, they are bland and 'neutral', capacious enough to embrace a variety of attitudes and lifestyles".[444] Yet, current sociological research can help in showing that shifting meaning does not equal loss of importance.[445] In keeping with the argument presented here, embracing wider understandings of family life (without lessening protection against the potential shortcomings of unleashed private power relations) can pave the way to greater autonomy, as is the case of same-sex couples and the termination of abusive relationships. The words of a recent ECtHR judgments could support this view, in particular "…The State, in its choice of means designed to protect the family and secure respect for family life as required by Article 8, must necessarily take into account developments in society and changes in the perception of social, civil-status and relational issues, including the fact that there is not just one way or one choice when it comes to leading one's family or private life".[446]

---

[441] Council of Europe (1956), Preparatory Work on Article 8 ECHR.

[442] For the CJEU, protection of the family has been instrumental in eliminating "obstacles to the exercise of the fundamental freedoms guaranteed by the Treaty" (Judgment of 12 May 2011 in Runevič-Vardyn and Wardyn, C-391/09, EU:C:2011:291, para 90.). The CJEU also noted the negative impact of freezing of funds on family life (*Judgment of 6 June 2013 in Ayadi v. Commission, C-183/12 P, EU:C:2013:369*, para 68.). The ECJ adjudicated on family issues also in the context of cooperation in civil matters. There, it ruled that the determination of what constitutes 'family environment' can be linked with the concept of habitual residence (Judgment of 22 December 2010 in Mercredi, C-497/10 PPU, EU:C:2010:829, para 56.).

[443] See Judgment of 25 July 2008 in Metock and Others, C-127/08, EU:C:2008:449, paras 62-64.

[444] Stephen David Coutts, 'Union Citizenship and the Area of Freedom, Security and Justice' (PhD thesis, European University Institute 2015).

[445] With reference to the American case, Hattery and Smith note that the evolving understanding of what family means does not subtract from its importance. Mary Ann Glendon, *The Transformation of Family Law. State, Law and Family in the United States and Western Europe* (The University of Chicago Press 1989) p. 145.

[446] Hattery and Smith (2013).

3.3.1.3 The right's third limb: home

As clarified in the case of family life, I revise the value of home in relation to my main argument, i.e. its support to personhood, identity and autonomy as the quintessential function of the right. Moreover, it should be immediately clarified that the typical understanding of respect for home in article 7 of the Charter concerns its inviolability, rather than the right to a home (which would fall within social rights). As a result of such restricted focus, the applications of the four-step methodology (the factors that enhanced the appearance of this limb of the right (1), and that challenged them (2); and on the other hand, the mechanism that favoured a legal approach to the concept (3) and the political occurrences that subsequently spurred its recognition as a right (4)) is necessarily less extended.

The home is typically the seat of the household,[447] where private and family life takes place (although not solely, as the case law of the ECtHR shows). For Arendt, home, in the sense of possessing (owning) one's private space, may actually be the only ancient Greek legacy retained as it was in today's concept of privacy.

Edward Coke's famous statement "A man's home is his castle – for where shall he be safe if it not be in his house?" (sometimes said to originate in ancient Rome) has turned home into a safe haven against public power (authority). The origins of such a conception of the home connect to trespass of chattels and the Castle Doctrine.[448] In this sense, the home was the first to acquire legal protection, even before the legal discovery of privacy. The *travaux préparatoires* of article 12 UDHR testify to how several countries had granted constitutional protection to the inviolability of the home before the adoption of the Declaration [1, 4]. [449]

The possibility for the home to become the place where one can also enjoy private and family life by hiding from the public eye (the social) is more recent, as it depends on the concrete availability of seclusion [1].[450] Suffice to note here that for the very large majority of the population the availability of seclusion is connected to sociological and demographic changes: the shrinking of the family; the improvement of standards of living and better

[447] As opposed to the house, which is generally regarded as simply a building. Mihaly Csikszentmihalyi and Eugene Rochber-Halton, The meaning of things. Domestic Symbols and the Self (Cambridge University Press 1981). Chapter V of the book contains an ethnographic study on the importance of the home or domestic environment for the self.

[448] The writ of habeas corpus (protection against illegal deprivation of liberty) could be seen as a logical antecedent of the protection of the home, as individuals needed first to be granted physical protection. However, to establish such a link, more research is needed.

[449] Johannes Morsink, *The Universal Declaration of Human Rights: Origins, Drafting and Intent* (University of Pennsylvania Press 1999).

[450] The article of Warren and Brandeis is a case in point.

dwellings; more affordable heating and lighting allowing people to spend time in separate rooms; and the appearance of modern bathrooms that changed hygienic customs into private rituals.[451] Currently, there seems to be a recrudescence of the high-density cities that hindered seclusion, where people live close together, creating 'qualified privacy' because the buffers between individuals' dwellings are removed [2].[452]

The importance of both conceptions of home has been once more highlighted by dictatorial practices in the 20th century in Europe. The extensive use of indoors/covert surveillance and expropriations were both ways of removing the protection afforded by the home. The first allowed at once finding out dissenters and instilling the Orwellian fear of being constantly checked, today referred to as the 'chilling effect', whereas the latter was a way of socializing non-conforming individuals.[453] However, the dictatorial experiences may have played a lesser role, given that the entitlement to the protection of the home had already gained legal protection. Nevertheless, currently the inviolability of the home is apprehended as part of the wider reasoning on private life, as the ECtHR noted recently in the case of *Stolyarova v Russia*, where the ECtHR found that "the margin of appreciation in housing matters is narrower when it comes to the rights guaranteed by Article 8 [than it is for those guaranteed by in Article 1 of Protocol No. 1], because Article 8 concerns rights of central importance to the individual's identity, self-determination, physical and moral integrity, maintenance of relationships with others and a settled and secure place in the community".[454]

The understanding of the home as a safe haven from public authority and from society may be challenged by information and communication technologies, for instance in the form of self-surveillance;[455] the extent to which individuals will embrace self-surveillance could testify to an important paradigm shift.

---

[451] Peter Ward, *A History of Domestic Space: Privacy and the Canadian Home* (University of British Columbia press 1999).
[452] Ibid.
[453] Arendt (1960), 'Freedom and Politics'.
[454] Stolyarova v. Russia, n. 15711/13, CE:ECHR:2015:0129JUD001571113, para 139.
[455] Michele Rapoport, 'Domestic Surveillance Technologies and a New Visibility' in Elisa Orrù, Maria Grazia Porcedda and Sebastian Volkmann (eds), *Surveillance and control beyond the security v. privacy model* (Nomos Verlag forthcoming).

3.3.1.4 The right's fourth limb: (Confidential) communications

Perhaps the value of communications, which encompass every form of spoken and written interaction, is the most self-explanatory: it is our primary tool of interaction and exchange, the way we express our needs and ourselves. Arendt[456] reminds us that communications play an important role in intimacy: expression modulates intimacy, to the extreme point that, once uttered, certain experiences lose their individual character altogether (as in the case of pain[457]). It is also crucial in the construction of the self.[458] If identity building is a relational process, and relationships are partly substantiated through language, then communications and language[459] must have always been relevant in this respect. Perhaps it is for the immediate appeal of communications and strong relation with intimacy that eminent scholars identified privacy with the control over knowledge about oneself.[460] Although I agree with Reiman's[461] rebuttal of that equation, it must be kept in mind that control over knowledge about oneself is part of the legal right of the definition, particularly ensuring the confidentiality of communications. Confidentiality can be described as the ability to ensure that a message and the information contained therein reach the intended recipient(s) only.

Similarly to the previous two sections, here I approach the value of communications in relation to its support of personhood, identity and autonomy as the quintessential function of the right. As before, the specific needs embodied by communications have acquired legal significance through a series of enhancing and limiting factors.

As for the enhancing factors, the link between communications and identity has been made explicit since Romanticism, when the creation of the self through expression and language was bridged through art. Uniqueness turned being true to oneself, i.e. creating oneself against constraining moral codes and the demands of other, into a goal in itself [1].[462] It follows that the expropriation of one's communications, through recourse to surveillance of any kind, or the threat thereof, can prove particularly harmful for the creation of the individual's image of the self [2].

---

[456] Arendt (1998), *The Human Condition*.
[457] For Arendt (1998), the act of uttering one's pain detaches the experience from the individual, removing its intimacy.
[458] Taylor (1989), *Sources of the Self*.
[459] Ibid.
[460] Westin (1967); Fried (1984).
[461] Reiman (1984), 'Privacy, Intimacy and Personhood'.
[462] Taylor (1989), *Sources of the Self*.

If the environment does not offer reassurances of confidentiality, forms of cryptography are used. This introduces the first encounter with techniques and technology, which in this case acts as a protective element. The attempt to infuse communications with confidentiality through (increasingly sophisticated) cryptography for political or other reasons has existed since antiquity, as much as interception for political needs, as exemplified by the surveillance undergone by one of Italy's founding fathers, Mazzini[463] (in this case, technology is part of the methods to counter the offences and achieve the desired notion of security). In this respect, fascist and totalitarian regimes have not particularly 'excelled', in that the violation of private correspondence is certainly not their invention.[464] Nor does the temptation to violate communications confine itself to dictatorial regimes, as Snowden's revelations remind us. While by no means constituting the only relevant technological development, information and communication technologies (from the telegraph to the Internet) are associated with the tools enabling the deepest intrusion. And yet, confidential communications stand out as one of the entitlements most cherished throughout Europe's history.[465] I will come back to the confidentiality of communications in chapters 3 and 4.

3.3.2 Giving normative-legal value to the right to the protection of personal data (art. 8 of the Charter)

Article 8 reads

> *"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."*

[463] Lepore (2013).
[464] David Kahn, 'Back When Spies Played by the Rules' *The New York Times* (13 January 2006).
[465] Ibid.

Data are understood as pieces of raw information that concern an identified individual, or that enable her identification[466] (on the legal understanding of data and information, see chapter 4).

Similarly to that done for the right to private life, this section intends to show the value of personal data protection enshrined in article 8 of the Charter, by reasoning on the historical conditions of its appearance, due to the scant clues contained in the *travaux préparatoires* to article 8 of the Charter.[467] In doing so, I draw on the work of several 'privacy' scholars. In what follows I also undertake a law and society approach to give back value to the right, but with a slightly different approach than that followed for the right to respect for private and family life, in that I detach accounts on the appearance of the notion from its value. This is an intentional choice, because I want to describe its value *vis-à-vis* the right to private life in order to differentiate the two. I begin by referring to the historical progression leading to the adoption of the right, in the context of which I highlight the four moves described above: the factors that enhanced the surfacing of the existence of the concept of personal data [1a], and that challenged its protection [2]; and the mechanism that favoured a legal approach to the concept [3] and the political occurrences that subsequently spurred its recognition as a right [4]. Then, I move onto describing personal data protection's value [1b], as partly in synergy with and partly different to private life.

3.3.2.1 The emergence of the notion of personal data protection

Westin's point, whereby a new need enters the realm of freedom when it is both enhanced and challenged, applies to personal data protection. As above, I believe a brief account of the mechanisms at play is instrumental in better grasping the value of the right.

The appearance of the notion of personal data is certainly related to the ability of the state to collect encompassing information on its citizens for the purposes of censuses, and the implementation of public welfare measures.[468] But the invention of computerized systems and the unprecedented (personal) data processing capabilities they enabled perhaps plays the

[466] Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data* (01248/07/EN WP 136, 2007).
[467] Lynskey (2015).
[468] Rodotà (1973), *Elaboratori Elettronici e Controllo Sociale*.

biggest part. González Fuster[469] notes that in the original version of 'data protection' – the German *datenschutz – daten* indicates data processed by a computer system, rather than raw information. A relatively small invention, the so-called 'search function,' which allowed selecting the desired words or portion of content in a text, led to impressive business opportunities, notably building searchable, refined databases for both the public and private sectors. [470] This in turn enabled the development of a fundamental feature: the (trans-border) 'flows' of personal information, whereby data containing personal information were exchanged, point-to-point, to support bureaucracy, to supply national and international businesses (shipping, travelling), or as a business itself (e.g. marketing) [1a].

Yet, those same developments would soon show their problematic face. Simitis[471] recalls how the early debate on computers was dominated by figures like Norbert Wiener (the father of Cybernetics) and Frank, who saw in 'cybernetic machines' a way to rationalize society, allowing objective decisions to be taken (see chapter 3). The enthusiastic approach that led to building the databanks of the Land of Hessen in the mid-60s cooled down when the surveillance capabilities of processing the health and income-related data of most of the population of the Land started being questioned [2]. The outcome was the adoption of the Data Protection Act of the State of Hessen in 1970. The act was able to benefit from earlier discussions in the US Congress,[472] based on Westin's work,[473] taking place between 1966 and 1968. The interaction of the uncovering of surveillance-related scandals,[474] and the adoption of pioneering legal instruments, triggered comprehensive academic and legal reflections on the possible impact on human rights, at the time expressed in terms of privacy, and the establishment of international thematic commissions producing reports, studies, and international declarations, such as the United Nations' 1975 Declaration.[475]

It was the opposing needs of profiting from the market potential of the flow of data, and the dangers a wild flow could provoke, which pushed the matter into the legal realm [3]. The US spread the successful legacy of Fair Information Principles (hereafter FIPs), standards to

---

[469] González Fuster (2014).
[470] Johan Eriksson and Giampiero Giacomello, 'Content Analysis in the Digital Age: Tools, Functions, and Implications for Security' in Sandro Gaycken and Jörg Krüger (ed), *The Secure Information Society: Ethical, Legal and Political Challenges* (Springer 2012).
[471] Simitis (2010).
[472] Ibid.
[473] González Fuster (2014).
[474] Newman (2008); Rodotà (1973), *Elaboratori Elettronici e Controllo Sociale*.
[475] United Nations, General Assembly, *Declaration on the Use of Scientific and Technological Progress in the interest of Peace and for the benefit of Mankind (Teheran Declaration)* (Thirtieth Session, 2400th plenary meeting, 1975).

treat information fairly and avoid unwelcome effects while benefitting from the flow of data.[476] Firstly applied in the US in the 1974 Privacy Act and further refined in 1977, FIPs informed the Privacy Guidelines of the OECD[477] and Convention 108,[478] both of which use the expression 'privacy' to refer to the protection of personal data. Though with diverging choices, both instruments dealt with the need to reconcile the smooth trans-border flow of personal data (in light of their increasing economic importance) with the protection of the individuals concerned. The advent of the information society has exacerbated such tension, to the point that, depending on the preferred reading of article 8, the flow may have acquired the role of intrinsic balance to the protection of personal data.[479]

Supra (section 3) I mentioned that the EU originally took an instrumental approach to data protection. The EU began addressing the matter around 1973 to harmonize Member States' approaches and at the same time counter the commercial and legal dominance of the United States in the field.[480] While Convention 108 was initially deemed sufficient to address personal data protection, it was the adoption of the Schengen Convention that spurred the need to adopt more substantial legislation at Member States' level and, in the face of the lack of harmonization and the waxing information society, a Directive.[481] The inclusion of article 8 in the Charter, which paved the way for the end of an instrumental approach to data protection, was the modernising result[482] of the favourable presence of several 'personal data protection' activists among the members of the drafting Convention [4].[483] Thus far, I have referred only indirectly to the value embodied by the right, to which I turn in the following two paragraphs.

[476] Gellman (2012).
[477] OECD Privacy Guidelines.
[478] Convention 108.
[479] González Fuster (2014).
[480] Ibid.
[481] Martin Bangemann and et al., *The 'Recommendations to the European Council. Europe and the global information society'. The Bangemann Report* (1994).
[482] Piris (2010).
[483] González Fuster (2014).

3.3.2.2 Personal data bearing value in synergy with private life, with a twist

I agree with González Fuster[484] that modern information technology, although crucial, is insufficient alone to explain the elevation of personal data protection to a right [4]. In part, the right aims to protect the same values underpinning private life: the two rights meet at the intersection of identity, autonomy and dignity [1b]. I see this relationship as one of synergy, rather than of the dependence of personal data protection on private life.[485] This holds true also in the partly related case of personal data embodying information concerning the private life of the individual,[486] from which I begin my discussion.

Whenever personal data contain information that allows reconstructing details about the private life, social circles or communications that individuals would rather keep private, there is a clear and manifest overlap between the object the two rights seek to protect, which usually is intimacy (individual and relational) functional to personhood and identity. In this case the only difference that could be traced is the one found by Rodotà.[487] That is, on the one hand, the right to private and family life tends to be static, in that it relates to the physical and spatial dimension of the individual. On the other hand, according to Rodotà, the right to personal data protection is dynamic, in that it refers to data by their nature detached from the person and susceptible to flow. In this respect, protecting personal data equals stepping up protection of intimacy; this is a possible reading, for instance, of *Google Spain's* 'right to be forgotten'[488] (see chapter 7).

A second, connected point of overlap concerns the fact that both rights aim at keeping solid control of the process overseeing the creation of one's identity (and, relatedly, dignity and autonomy). If we agree that information concerning intimacy is itself an integral part of intimacy, and we accept that gatekeeping one's intimacy is required to foster the creation of independent identities, then gatekeeping one's intimate information (of which Westin's notion

[484] Ibid.
[485] For a similar conclusion, see Tzanou (2012). She argues that, even if the right to personal data protection may serve to a large extent the 'right to privacy', it also fulfils different objectives.
[486] While I agree with Lynskey's conclusion that the right to personal data protection should be treated as a fully-fledged independent right, I believe that the three models she uses to explain the origins of the right to personal data protection are complementary, rather than standing in opposition. First, there was a general rediscovery of personality rights based on dignity, on which I argue that private life rests upon; the appearance of personal data protection, serving similar purposes, was immediately linked to private life (just like private life had been linked to property rights); time proved the usefulness of having two rights which merit to be treated independently, but the common origin and purpose testify to an overlap.
[487] Rodotà (2009), 'Data Protection as a Fundamental Right'.
[488] Judgment of 13 May 2014 in Google Spain and Google, C-131/12, EU:C:2014:317.

of 'control' is an aspect[489]) is crucial for identity and, relatedly, autonomy. This was the sense of the landmark judgment pronounced by the German Constitutional Court in relation to the regulation of census, and which was crucial in the construction of a European culture of the protection of personal data. In 1983 the Court claimed that individuals have a "right to informational self-determination" deriving directly from article 1 (1) and 2 (1) of the German Constitution (the Basic Law), whereby the rights to freedom are inviolable.[490] The judgment reads

> *"Those who cannot understand with sufficient certainty which information related to him or her is known to certain segments of his social environment, and who is not able to assess to a certain degree the knowledge of his potential communication partners, can be hindered profoundly in their freedom of self-determination to plan and to decide. The right of informational self-determination stands against a societal order and its underlying legal order in which citizens cannot know any longer who knows what about them when and in which situations."*[491]

Having said that, I believe the two rights oversee the protection of identity differently, and Rodotà's distinction traced above can be useful to exemplify this. Individuals need a physical and emotional margin of manoeuvre, a material or ideal space where they can feel free to develop their personality; this is where the right to private life comes into play. Individuals, however, also need reassuring that, once that personality is expressed, its integrity can be protected against direct or indirect attempts to deny its richness and possibility to change; in this respect, I embrace the point, made by Tzanou,[492] that the purpose of protecting data concerns its processing. In a society preoccupied by the need to categorise the behaviour of individuals according to standards, for the sake of planning and regulating economic

[489] In similar criticism, Tzanou formulates the notion of 'informational autonomy' (Reiman (1984), 'Privacy, Intimacy and Personhood'; Reiman (1995), 'Driving to the Panopticon'.
[490] Poullet and Rouvroy (2009). "Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß." (retrieved here: http://www.servat.unibe.ch/dfr/bv065001.html). I am indebted to Sebastian Volkmann for this translation. A translation of fundamental passages of the Volkszählungsurteil case is available at: https://freiheitsfoo.de/census-act/.
[491] Volkszählungsurteil, 65 BVerfGE, 1, Bundesverfassungsgericht - German Federal Constitutional Courts, 15 December 1983, para 154.
[492] Tzanou (2012).

activities, and where behaviour is conditioned according to status (particularly the function or role undertaken[493]), profiling,[494] helped by big data[495] and information technologies in general, appears alluring. There has been no shortage of attempts to justify a commercialization of personal data based on the economic potential they carry, which, however, "ignore the full social costs of data use".[496] Profiling removes the power of individuals to make claims about who they are. Retaining control over personal data allows the individual to oppose being seen as a conditioned animal,[497] whereby association to a flat category crushes his or her richness. It could be useful in this respect to recall Reiman's[498] four risks entailed by the collection of personal data: the risk of extrinsic loss of freedom (the chilling effect), the risk of intrinsic loss of freedom (the actual limitation of the right), symbolic risks (impinging on the individual's ownership of oneself), and the risk of psycho-political metamorphosis (infantilizing adults, turning them into Marcuse's one-dimensional man).

Recital 75 of the GDPR acknowledges that: "… where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles", there is a "risk to the rights and freedoms of natural persons" which could lead to "physical, material or non-material damage". It is in this light that profiling of children is inadvisable, as they "may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data" (recital 38 of the GDPR).

[493] Article 4.4 of the GDPR defines profiling as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." See Arendt (1998), The Human Condition.

[494] Andreas Kuehn and Milton Mueller, *Profiling the Profilers: Deep Packet Inspection for Behavioral Advertising in Europe and the United States* (Syracuse University, School of Information Studies, 2012).

[495] Christopher Kuner and others, 'The Challenge of 'Big Data' for Data Protection' (2012) 2 International Data Privacy Law.

[496] Simitis (2010), p. 1999.

[497] Arendt (1998), *The Human Condition*.

[498] Reiman (1995), 'Driving to the Panopticon'.

3.3.2.3 The independence of personal data protection

There are instances, however, in which personal data embody information that does not immediately unveil details of one's private life. Kranenborg[499] and Lynskey[500] note that the ECtHR has systematically denied protection to such data, which instead fall within the purview of article 8 of the Charter.[501] The importance of protecting data is intimately linked to contemporary advances in information technology spurred by the Internet,[502] namely technological developments and new forms of crime.

Technological developments include cloud computing, big data and the internet of things. Cloud computing detaches the data from a physical location, [503] and once in the cloud, data is difficult to tame.[504] Big data[505] aims at stacking as much data as possible in unique databases (following the encouraging results of using large databases in science and meteorology) in the hope that producing vast haystacks will enable identifying the desired needles. Big data challenges the principle of purpose limitation and data minimisation (in that data are not collected and exchanged for limited purposes by known data controllers, and that there is an incentive to collect as many data as possible), which has triggered discussions about a new facet of the right to data protection, the right to be forgotten, or the ultimate deletion of one's data.[506] The Internet of Things merges the two approaches: everyday objects connect to the Internet and their information, stored in clouds, leads to ever-bigger data.

As for 'new' forms of crime (see chapter 3, section 3), personal data is also exposed to cybercrime and cyber surveillance, which begs the question of whether protecting data is akin to protecting information systems in accordance with the information security canons, a

[499] Herke Kranenborg, 'Access to Documents and Data Protection in European Union: on the Public Nature of Personal Data' (2008) 45 Common Market Law Review 1079-1114.
[500] Lynskey (2015).
[501] Kokott and Sobotta (2013).
[502] Stefano Rodotà, *Il Mondo nella Rete. Quali i Diritti, Quali i Vincoli* (Editori Laterza 2014).
[503] Michael Armbrust and others, *Above the Clouds: A Berkeley View of Cloud Computing.* (Technical Report No UCB/EECS-2009-28, 2009).
[504] Claire Gayrel and others, *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 2010) <<http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1b.pdf>>.
[505] Omer Tene and Jules Polonetsky, 'Privacy in the Age of Big Data: A Time for Big Decisions' (2012) 64 Stanford Law Review Online.
[506]See in this respect *C-131/12 - Google Spain and Google*.

question addressed by the German Constitutional Court, which I discuss in greater details in chapters 3 and 4.[507]

The bottom line of such dramatic and entrenched developments of informatics is manifold. First, technology acts both as a challenge to the protection of personal data, and as a potential solution, expressed particularly in the notions of privacy enhancing technologies (PETs), i.e. technologies that pursue the objective of protecting privacy rights, and Privacy by Design, the brainchild of Ann Cavoukian, which aims at embedding considerations of privacy rights in the design phases of technologies.

Second, it is not possible to anticipate the ways in which personal data can be used. Hence the rationale of a right: all personal data deserve protection irrespective of the immediate danger posed by their processing. However, in order to accommodate legitimate processing (which "should be designed to serve mankind", recital 4 of the GDPR), the exact technical, organizational and legal measures enacted to safeguard data will depend on the assessment of the (known) risk posed by the processing, according to a well-established risk-based approach.[508] The GDPR refers to generic risks, significant or high risks to the rights and freedoms of natural persons, which may lead to physical, material or non-material damage (recital 75), as well as data security risks (recital 83) (further discussed in chapter 7, section). If fully anonymised data are not considered personal data any longer, pseudonymised data (article 4(5) of the GDPR) pose low risk. So-called sensitive data pose significant risks (recital 51), whereas high risks are those that follow a specific assessment, e.g. in relation to data breaches or new technologies (see chapters 4 and 7). By means of example, recital 75 indicates the risk of discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, a significant economic or social disadvantage, the deprivation of the exercise of one's data rights, the processing of special categories of sensitive data and of vulnerable people, or on a large-scale basis.

Thirdly, personal data collected for different legitimate purposes can be crossed without consent to lead to decisions that affect the individual in very material ways. It is not a chance that both the GDPR and the revised Convention 108 insist that automated decisions, i.e.

[507] For a similar conclusion, Tzanou (2012).
[508] E.g. Article 29 Data Protection Working Party, *Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks* (14/EN WP 218, 2014).

decisions that do not involve human agency, undergo heightened controls.[509] Decisions based on automated processing stem from a partial depiction of the individual, which is based on the expropriation of the control over identity and (digital) personality. Recital 71 of the GDPR recommends such decisions not to concern a child (in the GDPR, a child aged 13 or under), and offers examples of the negative effects of such decisions on the data subject, e.g. "automatic refusal of an online credit application or e-recruiting practices without any human intervention".

To act differently would lead to a loss of autonomy, but in a subtler, and thus more dangerous, way.[510] It is for this reason that it is crucial to safeguard 'the digital/electronic persona'[511] as distinct from the physical persona,[512] needing specific legal protection, substantiated in procedural rights safeguarding the use of personal information, as indeed is the case of paragraph two and three of article 8 of the Charter.[513]

In this respect, personal data protection can be assimilated to a procedural right akin to non-discrimination, understood as a measure of accessibility,[514] other than availability, of goods and services. Its function is to prevent individuals suffering from a spiral of other human rights infringements, including but not limited to the right to private and family life, as well as affecting the realization of a substantive right (such as freedom of expression, association, and movement, which could not be effectively enjoyed otherwise).

Certainly it will be for the CJEU to provide a final answer on the independence of personal data. The CJEU could rely on article 52.2 of the Charter concerning rights derived from the Treaties (as could be the case for personal data protection). Furthermore, the Court's adoption of definitions contained in secondary law could play to the advantage of article 8. The new GDPR, in fact, does not formulate rules on personal data protection in subsidiary terms to

---

[509] European Parliament, Mady Delvaux (Rapporteur), *Draft Report with Recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103 (INL), 2016).

[510] "The digital persona is a construct, i.e. a rich cluster of inter-related concepts and implications…" defined as "A model of an individual's public personality based on data and maintained by transaction, and intended for use as a proxy for the individual". Arendt (1998), *The Human Condition*.

[511] Roger Clarke, 'The Digital Persona and its Application to Surveillance' (1994) 10 The Information Society.

[512] On the relevance of the second paragraph of the article to trace a neat line between article 7 and 8, see also Kokott and Sobotta.

[513] Rodotà (2009), 'Data Protection as a Fundamental Right'.

[514] For a similar conclusion, United Nations (2012). Tzanou discusses the possibility that data protection may act like non-discrimination in relation to profiling, whereas Poscher and Miller argue that the right to informational self-determination is anticipatory in nature, in that it "anticipates a potential harm resulting from the collection, storage and use of personal information". Ralf Poscher and Russell Miller, 'Surveillance and Data Protection in the Conflict between European and American Legal Cultures' (2013) <http://www.aicgs.org/issue/surveillance-and-data-protection-in-the-conflict-between-european-and-american-legal-cultures/>; Tzanou (2012).

private life. In this respect, the CJEU may follow the same approach of *Fisher*,[515] by embracing the Regulation's formulation before it enters into force.

3.3.3 THE VALUE OF ARTICLES 7 AND 8 FOR THE EU ORDRE PUBLIC

Fascist and totalitarian regimes demonstrated the dangerous consequences of crushing the four dimensions of the legal definition of the right to respect for private and family life discussed in this article, to the extent that "the rise of totalitarianism…its consistent non-recognition of civil rights, above all the right to privacy, makes us doubt not only of the coincidence of politics with freedom, but their very compatibility".[516] Reiman recalls Goffman's studies concerning the impact of total institutions on the self, whose mortification of the self passes through the removal of any privacy."[517] Totalitarian regimes crushed private and family life, home and correspondence with the use of ideology and terror, with a view to curbing the individual's spontaneity and leeway for action, and substituted autonomy with automatic processes.[518] By stifling spontaneity of political action (what Arendt called Machiavelli's virtù),[519] regimes[520] would neutralize the possibility to effect social change.

The same could be argued about personal data. The physical elimination of 'the enemy' during (but also after) WWII was often achieved through (compiling) lists of dissidents and ethnical or religious affiliations. It was perhaps the 20th century dictatorial regimes in Europe and government reactions to the Cold War that showed the widest consequences of the collection of personal data, which lead to categorizing individuals between friends and foes, chilling the autonomy of the former and seriously imperilling that of the latter.

Our modern democracies are founded on the (ideal) notion of the autonomous citizen endowed with a unique identity, worthy of equal respect because of his or her intrinsic dignity, who retains liberty, the freedom to act politically, at a minimum through voting, and the prerogative to request the correct application of the rule of law. The ECtHR pronounced

[515] *C-369/98 - Fisher*.
[516] Arendt (1960), 'Freedom and Politics', p. 30.
[517] Reiman (1984), 'Privacy, Intimacy and Personhood', p. 310.
[518] Arendt (1960), 'Freedom and Politics'.
[519] Ibid.
[520] Cohen (2013) compellingly argues that this is not only the case of political regimes, but also of democracies and liberal economies based on modulated surveillance. See also Poullet and Rouvroy 2009.

that "although no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees" including "a right to personal development".[521] A polity based on the (ideal of the) rule of law is a polity of autonomous citizens,[522] as supposedly is the EU pursuant to its Treaties.

Independent identities enabling autonomy cannot be developed without enjoying the four limbs enshrined in article 7 of the Charter, because "privacy prevents interference, pressures to conform, ridicule, punishment, unfavourable decisions, and other forms of hostile reaction. To the extent that privacy does this, it functions to promote liberty of action, removing the unpleasant consequences of certain actions and thus increasing the liberty to perform".[523] Similarly, independent identities cannot be developed without the enjoyment of personal data protection, which protects individuals from being infantilised[524] and seen as a conditioned animal[525] (*supra*, section 3.2.2.2).

It would be foolish to rely on the work of the past to enjoy such prerogatives if the understanding of their significance is not kept alive, particularly in the face of the repeated challenges of terrorism. But it would also be foolish to believe that we could afford indifference if and when the terrorist threat is over. In her essay, Cohen argues about the dangers of sleepwalking in a modulated democracy, where we allow the creation of surveillance infrastructures that organize the world for us, force us to look at the world through their lenses, and that are ultimately exploited "by powerful commercial and political interests".[526]

[521] *Pretty v. the United Kingdom, n. 2346/02*, para 61.
[522] Bobbio (1997). Reiman lists four risks, recalled *supra*, section 3.3.2.2, p. 98. Gavison (1984), p. 363-364.
[523] Reiman (1995), 'Driving to the Panopticon'.
[524] Ibid.
[525] Arendt (1998), *The Human Condition*.
[526] As powerfully forecasted by Cohen (2013), 1912.

4 CONCLUDING REMARKS

In this chapter I have appraised the trade-off model from a methodological perspective, whereby I have focussed on the first two steps of what I called the 'methodological challenge' (hypothesis I).

First, I looked at the legal meaning of 'security' and 'privacy' in the EU legal order, and underlined the inability of these terms to explain all dynamics at play, notably because of the important role of technology, neglected by the trade-off. The analysis has shown that, in legal terms, references to security should be substituted by references to specific offences. Such an analysis has also shown the inconsistency of the term 'privacy' in the EU legal order, where the notion is covered by two rights having equal standing: the rights to respect for private and family life and to the protection of personal data. Both rights are nuanced and their facets embody different values. Both rights are important to preserve our system as a democracy based on equally respected individuals, as endowed with dignity, whose freely developed identity and personality informs the autonomy necessary to participate in the system, enjoy other fundamental rights, and take action to ensure that the safeguards overseeing the desired functioning of the system – the rule of law – are properly in place. The foundation of such democracy is the individual, not the group, as much as human rights are (mostly) about the individual, not the group.

Second, I noted that the trade-off fails to acknowledge the importance of a hidden variable, that of technology. I noted in particular that, together with substituting the vague notion of security with specific offences, we should also look at the technologies used to prevent, investigate and prosecute them. Hence, using the case of terrorism as an example, I have proposed reformulating the simple 'trade-off' as a more complex relationship: "using the method/tool X to combat (prevent) the 'seizure of aircraft, ships or other means of public or goods transport' at the expense of a specific limb of the right to private life, which enables intimacy". Such a reformulation shows the inconsistency of a security measure ostensibly for protecting a society based on the autonomous and unique individual! Unless, of course, we are facing an epochal paradigm-shift. Later in the chapter, however, I noted that technology is also a hidden variable of the two privacy rights, which not only encroaches on them (irrespective of the fight against crime), but also safeguards them.

As a result, when thinking of the reformulation of the trade-off, it is interesting to think about the fact that technology could also be placed on the second part of the equation. This reflection will be developed in chapter 4 in the context of cybersecurity, together with reflections on the efficiency of trading-off security with privacy rights (and hypothesis I). The reason is that such a reflection can be meaningfully carried out only in relation to concrete technologies. The next step will be to obtain suitable reformulations of the trade-off in the context of cybersecurity, my case study and the object of the next chapter.

CHAPTER 3 - CHALLENGING THE TRADE-OFF: THE CASE STUDY OF CYBERSECURITY

"If, as Sardar and others suggest, 'cybercrime is going to be the crime of the future', then rather than bringing to mind the new Jerusalem, one might wonder if cyberspace will be more like a new Gomorrah"
Margaret Wertheim[527]

This chapter focuses on cybersecurity as a case study of the trade-off between security and privacy rights. Herein, I apply the normative and methodological challenge I developed in chapters 1 and 2, with a view to ascertaining whether the pursuit of cyber-security can be reconciled with the rights to private and family life, and the protection of personal data. Thereby, I wish to develop previous work of mine[528] and of those authors that vouch for a convergence between cybersecurity and privacy rights.[529]

Section one has two goals. First, I spell out the reasons why cybersecurity is an interesting case from the perspective of the trade-off model. Second, I show how trading-off privacy rights with security in the context of cybersecurity can be criticized on the same grounds used in chapter one, which I termed 'the normative challenge'. The discussion shows the inconsistency of an abstract discussion and the need to move to a more concrete plane, i.e. that of the methodological challenge: appraising the concepts of cybersecurity and cybercrime in the context of specific measures.

Section two functions as a buffer between the normative and the methodological challenge. There, I sketch the EU policy approaches to cybersecurity from the angle of its interaction

[527] Margaret Wertheim, *The Pearly Gates of Cybersapce. A History of Space from Dante to the Internet* (W. W. Norton & Company Inc. 1999) p. 298.
[528] Chiefly Maria Grazia Porcedda, 'Data Protection and the Prevention of Cybercrime: a dual role for security policy in the EU?' (LL.M. thesis, European University Institute 2011).
[529] See, for instance, Peter Swire and Lauren Steinfeld, 'Security and Privacy After September 11: The Health Care Example' 86 Minnesota Law Review; Landau (2010), *Surveillance or Security*; Helen Nissenbaum, 'When Computer Security meets National Security' in Jack M. Balkin (ed), *Cybercrime, Digital Cops in a Networked Environment* (New York University Press 2007); Lee Tien, 'Architectural Regulation and the Future of Social Norms' in in Jack M. Balkin (ed), *Cybercrime, Digital Cops in a Networked Environment* (New York University Press 2007); Mary De Rosa, *Data Mining and Data Analysis for Counterterrorism.* (Center for Strategic and International Studies, 2004). In their essay, Drewer and Ellerman underline how good data protection rules can support good cybercrime investigations. Daniel Drewer and Jan Ellermann, 'Europol's Data Protection Framework as an Asset in the Fight against Cybercrime' (Joint ERA-Europol conference Making Europe Safer: Europol at the Heart of European Security, The Hague, 18-19 June 2012).

with policies concerning privacy rights. This defines the scope of the methodological challenge, which, it should be remembered, is inherently jurisdiction-specific.

Hence, section three contains the methodological challenge to 'cybersecurity v. privacy rights'. As anticipated in chapter 2, I will be focussing on the first of the three steps, which consists in analysing the meanings of 'cybersecurity', and 'cybercrime' in the context of Union law and policy. The analysis of those terms will show their meaning changes depending on the sub-area in which they are used, and enables substituting 'security v. privacy' with more complex and nuanced relations. The second and third steps will be dealt with in chapter 4, in relation to concrete technologies.

1 THE CASE STUDY OF CYBERSECURITY AND THE NORMATIVE DESIRABILITY OF RECONCIALITION

The criticism of a trade-off model in cyberspace can be rejected on the same grounds identified in chapter 1 (section 1). The normative challenge offers the opportunity to reflect on the peculiarity of cybersecurity, and explain why it is a particularly interesting case to study the trade-off model. The discussion will show the inevitable inconsistency of an abstract discussion and the need to appraise the issue on a concrete plane.

1.1 THE NORMATIVE CHALLENGE APPLIED TO CYBERSPACE: PRIVACY RIGHTS SHOULD NOT BE TRADED-OFF WITH CYBERSECURITY

In chapter one I challenged Vermeule and Posner's thesis on three mainly normative grounds: trading-off security with rights belongs in a wider theory of politics and the law; the EU is founded on the premise that governments can be dysfunctional (or worse) and must be reined in; and EU political choices are constrained by its *ordre public* built on the rule of law

(a fourth ground concerned the notion of emergency). These three grounds are of use to support the idea that security and privacy rights should be reconciled in cyberspace, too.

First of all, as Dunn Cavelty aptly observes, "cyber-security is a type of security that unfolds in and through cyberspace; the making and practice of cyber-security is both constrained and enabled by this environment."[530] It should be recalled that, despite its literary origins,[531] 'cyberspace' is now commonly used not just in academia, but also in official settings (though not in legal terms),[532] and should be therefore treated as the object of serious analysis. Cyberspace is widely defined as the interaction between technology and the human relations occurring thanks to this technology, as exemplified by Ottis and Lorents' definition of cyberspace as "a time-dependent set of interconnected information systems and the human users that interact with these systems".[533] The human element, which makes room for law and regulation, may actually be inherent in the notion of space: Wertheim[534] highlights that notions of space correspond to conceptualizations of the individual, whereas Dunn Cavelty[535] reminds us that space calls for dominance and control.

Moreover, I agree with Leenes that technology is never 'neutral',[536] particularly in cyberspace, but is rather pulled by diverse human purposes, the conflicting values they express, and the different normative systems of resolution available (and preferred). Hence, 'cyberspace' is an inherently political notion. At the Internet's inception, the Electronic Frontier Foundation's founder John Perry Barlow (who greatly contributed to the politicization of discourses on cyberspace[537]) presented it as a terrain independent from state

---

[530] Myriam Dunn Cavelty, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse' (2013) 15 International Studies Review 105, p. 107.
[531] The term 'cyberspace' is of literary origin, coined by the novelist William Gibson in 'Neuromancer', whereas 'cyber' comes from Norbert Wiener's cybernetics, which derives from the Greek 'kubernētēs, meaning 'steerman' (the word linked to 'govern*'). Rossella Mattioli, 'The 'State(s)' of cybersecurity' in Giampiero Giacomello (ed), *Security in Cyberspace* (Bloomsbury 2014); Wertheim (1999).
[532] For instance: European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, *Cyber Security Strategy: An Open, Safe and Secure Cyberspace* ((Joint Communication) JOIN (2013) 01 final, 2013); White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World* (2011); White House, *President's Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (2009).
[533] Rain Ottis and Peeter Lorents, 'Cyberspace: Definitions and Implications' (Proceedings of the 5th International Conference on Information Warfare and Security, ICIW). Cited in Mattioli (2014), p. 25.
[534] Wertheim (1999).
[535] Dunn Cavelty (2013).
[536] Because of its 'affordances', its ability to (intentionally or not) enable or inhibit behaviour. Ronald Leenes, 'Framing techno-regulation: an Exploration of State and Non-state Regulation by Technology' (2011) 5 Legisprudence.
[537] Dunn Cavelty (2013), p. 107.

bureaucracy, where likeminded people would pursue an egalitarian, peaceful utopia.[538] However, the success of the Internet brought about clashes of values and an ensuing proliferation of conflict. This includes the clash between the free enjoyment of rights and the attempts by either the state or users to limit such enjoyment (let alone the guarantees of those rights), clashes between rights, and different modes of governance of cyberspace (from no control to maximum control). Hence, different conceptions of (cyber) space correspond to different communities and modes of governance.[539] Consequently, the meaning of cybersecurity varies according to understandings of cyberspace, the values predominant in a given community and society at large, and the means of resolution of conflict. The Union (and its member states) is no different, and policy documents show the desire to infuse cyberspace with the values it pursues offline (*infra*, section 2).

Secondly, mass-scale surveillance programs like the ones unveiled by Snowden are a case in point of dysfunctional or malevolent governmental behaviour. Enabling the prevalence of unrestrained surveillance for the sake of security in cyberspace, including by 'exceptional access', betrays the foundations of the Union's *ordre public* discussed in chapter 1 (section 2) and enshrined in the TEU, TFEU and the Charter, whereby the action of the executive must be adequate, proportionate and non-excessive in respect to the fundamental rights guaranteed, because governments (and their representatives) can betray their mandate.

As a result, the policy and legal approach to cyberspace, including its security, should be governed by the 'ideal' tenets of the rule of law (chapter 1, section 2.3.1),[540] including obviously respect for fundamental rights. Trading-off privacy rights for cybersecurity would be against the Union *ordre public* built on the rule of law as discussed in chapter 1. Laws governing the security of cyberspace must address Union and Member States' positive and negative obligations to respect, protect and fulfil privacy rights as enshrined in the Charter,

[538] Indeed, the first cyber-enthusiasts saw cyberspace as the promised New Jerusalem whose 'pearly gates', substituted by ports and routers, are open to every human with an Internet connection, where no borders exist, and the messiness of bodily incarnation is substituted by the immateriality, and immortality, of bits and bytes. Based on the idea that "for a technology to be successful, a latent desire must be there to be satisfied" (p.30), Wertheim (1999) explains that cyberspace fulfils the psychological vacuum created by a scientific conception of the world where there is no space for spiritual matters because everything is physical.

[539] See Nissenbaum (2007), 'When Computer Security meets National Security'; Dunn Cavelty (2013); George Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance and Policy* (Palgrave Macmillan 2015); Maria Grazia Porcedda, 'Reviving Privacy: the Opportunity of Cybersecurity' in *Challenges and Opportunities of Online Entertainment. Proceedings of the 8th International Conference on Internet, Law & Politics Universitat Oberta de Catalunya* (UOC-Huygens Editorial 2012).

[540] I proposed an adaptation of the meaning of the RoL tenets in cyberspace in Maria Grazia Porcedda, 'Rule of Law and Human Rights in Cyberspace' in Patryk Pawlak (ed), *Riding the Digital Wave – The impact of cyber capacity building on human development, Report No 21* (European Union Institute of Security Studies 2014).

the ECHR and national constitutions. This also entails addressing the potential impingement on rights of laws applying to security in cyberspace, notably those on cybercrime.

But there is more to the typical tension between the full enjoyment of privacy rights in cyberspace and their lawful limitation for the sake of security-related matters. As the Parliamentary resolutions in reaction to the NSA scandals[541] (Introduction, section 1.3.3) seem to suggest, there could be complementarity between privacy rights and cybersecurity, thus reversing *in toto* the trade-off model and justifying the question "can there be complementarity between privacy and security in the context of cybersecurity?" Irrespective of the answer, cybersecurity appears to be a particularly interesting topic to study the trade-off model, as I sketch in the next section.

1.2 CYBERSECURITY: A JANUS-FACED CASE STUDY

Cybersecurity seems suitable for studying the trade-off model due to its inherent ambiguity, whereby the pursuit of cybersecurity appears to both shield and challenge privacy rights. An important element of such ambiguity is the technology of the Internet, i.e. a network of computers, i.e. at least two computers connected by a single technology, whereby connection means the ability to exchange information.[542] A quick analysis of such a technology is sufficient to raise serious doubts as to the adequacy of the trade-off model as an intellectual device (see chapter 4). In fact, as I anticipated in chapter two (section 3), the legal approach to privacy rights, and particularly that of personal data, has changed in parallel with the expansion of computing and the expansion of its applications. Legal issues concerning personal data became more pressing when a number of changes took place.

First, when the storage capacity predicted by Moore's law increased, which enabled to build larger databases (and cross-reference them). Second, when computers became personal and user-friendly thanks to graphical user interfaces (such as Windows), making them generative technology[543] (i.e. platforms for the creative writing of software), which enabled to increasingly store private information. Third, when computers became linked in networks

[541] European Parliament (2014), *Resolution on the US NSA Surveillance Programme*; Council of Europe (2015).
[542] Andrew S. Tanenbaum and David J. Wetherall, *Reti di Calcolatori (Quinta Edizione)* (Pearson Italia 2011).
[543] Jonathan Zittrain, *The Future of the Internet and How to Stop it* (Yale University Press 2008).

(functioning on the basis of a gentleman's agreement favouring flexibility, or reliability, over security[544] and replacing computers as the technology for operations[545]) and allowed the point-to-point data and communication transfers. Fourth, when, thanks to the creation of web indexing and easy interfaces for web search, a growing portion of the world population has started using the network of networks, a.k.a the Internet, contributing to the an economic boom based on the diffuse flow of data and communications; when the infrastructure was privatized,[546] and its new owners were left free to place profit above the security and privacy of users. Fifth, when the family of technologies connected to the Internet broadened to include mobile devices, great source of personal data but also increasingly "sterile appliances"[547] offering pre-packaged services on proprietary systems that cannot be modified (or even understood) by users, but which thrive on users' willingness to share personal information. And finally, when vital services for the society – critical infrastructure – were connected to and rendered dependent on the Internet.

All such changes, particularly those connected to the Internet, brought about the Information economy, generating value[548] that permeates interpersonal communications, the market, so-called critical infrastructure and national security. It is such interpenetration, alongside the architecture of the Internet, that has made computer systems and networks not only a field of innovation,[549] but also a palatable source of evidence. As increasing parts of our lives move online, so does crime.

1.2.1 Privacy rights v. Cybersecurity, and Data as evidence

Such crime can have national security and SIGINT import. For instance, the Internet offers would-be terrorists propaganda, information on how to manufacture explosive devices, how to affiliate to the extremist group of choice, interact with like-minded people and arrange

[544] Ibid; Tanenbaum and Wetherall (2011).
[545] Tanenbaum and Wetherall (2011).
[546] Maryam Dunn Cavelty, 'National Security and the Internet: Distributed Security through Distributed Responsibility' in Giampiero Giacomello and Johan Eriksson (eds), *Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State*, vol 11 (International Studies Review 2009).
[547] Zittrain (2008), p. 3. According to him, sterile appliances limit the potential for innovation while heightening opportunities for regulation.
[548] A measure of the value of a network is Metcalfe's law, and corresponds to the square number of its potential users, which describes all possible connections. Tanenbaum and Wetherall (2011).
[549] The interaction between architecture, economics and innovation has been addressed by Barbara Van Schewick, *Internet Architecture and Innovation* (MIT press 2010).

terrorist acts.[550] The Internet can also be a conduit and a target of military attack. Exploiting zero-days vulnerabilities (i.e. unknown vulnerabilities in software) proved a useful ally in hybrid (*infra*, section 2.3.3), state-sponsored attacks, from Stuxnet, (the US-Israeli malware that undermined the Iranian nuclear development programme)[551] onwards. These cases offer a hand to trade-off like approaches, whereby privacy rights are superseded by imperative national security concerns. Even if such a strong approach is not followed, and even if crime does not have immediate national security import, data are still needed to provide evidence for the fight against (cyber)crime.

Cybercrime, helped by the vulnerability and complexity of computer and information systems[552] (assumed to be constantly rising),[553] includes very different misdeeds, ranging from botnets and Trojan horses, to trolling and spear phishing (*infra*, section 3.3). In its policy documents, the Commission refers to estimates of the global damage of cyber insecurity, which reportedly amount to several hundred billion euros.[554] After years of difficulties in producing reliable figures on offences and their cost,[555] due to reporting issues[556] or the complexity inherent in measuring,[557] some official statistics are being produced. For instance,

[550] United Nations (2012).
[551] Evangelos Markatos and Davide Balzarotti (eds), *The Red Book. A roadmap for systems security research* (The SysSec Consortium: A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: Europe for the World 2013).
[552] See, among others, *Ross Anderson and Tyler Moore* 2006; *Maria Grazia Porcedda* 2012, 90; *Sommer and Brown* 2011.
[553] European Commission, *Contractual Public Private Partnership on Cybersecurity & Accompanying Measures. Accompanying the document Commission Decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research an innovation between the European Union, represented by the Commision, and the stakeholder organisation* (Staff Working Document) SWD (2016) 216 final, 2016).
[554] Ibid.
[555] In 2010 the EU proposed conducting an EU Security Survey by 2013, to collect statistics on cybercrime, and to adopt rules on the jurisdiction of cyberspace. European Commission, *Delivering an Area of Freedom, Security and Justice for Europe's citizens – Action Plan Implementing the Stockholm Programme* ((Communication) COM (2010) 171 final, 2010).
[556] Sources of data include police-recorded statistics, population-based and business surveys, victim reporting initiatives and technology-based cybersecurity information. According to the UNODC, none of these avenues is, alone, sufficient for reporting purposes, but their data can be crossed to produce estimates. United Nations, Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (UNODC/CCPCJ/EG4/2013/3, 2013), Annex 3. See also Nir Kshetri, *The Global Cybercrime Industry. Economic, Institutional and Strategic Perspectives* (Springer 2010); United Kingdom, House of Lords, *Personal Internet Security* (Science and Technology Committee, 5th Report of Session 2006-07 edn, 2007); Ross Anderson, *Security Engineering. A Guide to Building Dependable Distributed Systems* (Wiley 2008).
[557] Ross Anderson and others, 'Measuring the Cost of Cybercrime' in Rainer Böhme (ed), *The Economics of Information Security and Privacy* (Springer 2012). United Nations (2013), Annex 2.

the UK Office of National Statistics estimated that in 2015 5.8 million cyber incidents took place.[558]

Law enforcement agencies are on the back foot *vis-à-vis* the scale and diversity of the threat, and its jurisdictional hurdles (see *infra*, section 3). Public-private partnerships, whereby law enforcement agencies cooperate with private service/infrastructure providers to carry out operations, are becoming the (legally dubious) norm in cyberspace.[559] For instance, the Union has recently brought to life cPPP, under the H2020 programme, with the newly formed European Cyber Security Organization, which gathers representatives of industry and academia.[560] Equally, a City of London Police pilot project consists in partnering with law firms to bring cases against cyber offenders, which is to be tried in civil courts in the hope to appraise cybercriminals and recover illicit gains.[561]

1.2.2 PRIVACY RIGHTS & CYBERSECURITY

On these premises, and given the dependence of our society upon network and information systems, it is worth asking whether it is sustainable to secure cyberspace in a retroactive manner, or to exploit weaknesses to pursue military objectives. This forces us to reflect on the importance of securing data and networks upfront. That there could be complementarity between cybersecurity and privacy rights may not be *prima facie* surprising, especially if one focuses on the technology involved, i.e. network and information systems (as I detail in chapter 4). Information in computing is part of a system, and is expressed in bits and bytes or data. Data can express *anything*: information[562] that is personally identifying, or not. At the

[558] Alan Travis, 'Cybercrime Figures Prompt Police Call for Awareness Campaign' *The Guardian* (21 July 2016).

[559] The Venice Commission has raised doubts as to the lawfulness of ISPs' compliance with requests to provide data or plant malware on their servers. Council of Europe (2015). I covered the subject in Maria Grazia Porcedda, 'Public-Private Partnerships: A 'Soft' Approach to Cybersecurity? Views from the European Union' in Giampiero Giacomello (ed), *Security in Cyberspace: Targeting Nations, Infrastructures, Individuals* (Continuum Books, Bloomsbury Publishing 2014). See also Council of Europe, *Guidelines for the Cooperation between Law Enforcement and Internet Service Providers against Cybercrime, Adopted by the Global Conference Cooperation against Cybercrime* (2008).

[560] European Commission, *Commission Decision of 5 July 2016 on the Signing of a Contractual Arrangement on a Public-private Partnership for Cybersecurity Industrial Research and Innovation between the European Union, Represented by the Commission, and the Stakeholder Organisation,* (C(2016) 4400 final, 2016).

[561] Vikram Dodd and Damien Gayle, 'Police to Hire Law Firms to Tackle Cyber Criminals in Radical Pilot Project' *The Guardian* (14 August 2016).

[562] For Andrade (2011) information can be everything. Not only is information an intellectual cosmos, i.e. a system helping us to make sense of reality, it also corresponds to the cosmos, in the sense of constituting the

same time, data carry *anything*, irrespective of meaning, in the form of signals. Hence, data represent the link between information (the logical layer) and the network (the physical layer): they are the vector transporting information, in the shape of bits and bytes, via networks. The networks or physical layer[563] is made of the communication channels that enable the material delivery of information (just like trucks, ships and airplanes within a postal system). Communication channels in the physical layer are not optimized for the applications using them (as is otherwise the case of conventional telecoms), which led Isenberg to describe the Internet as a "stupid network",[564] whereby the intelligence is situated in the machines that originate the data flow, the centre of the network is based on infrastructure, and transport follows the need of data rather than constraints of the network. Accordingly, data are transported in packets in accordance with layering and the end-to-end argument, whose broad version generates 'net neutrality' viz. delivery follows best efforts regardless of the content carried.[565]

Since data flow from equipment ultimately operated by persons, the information carried by networks (whether or not publicly available electronic communications systems) in the form of content, traffic or location data[566] can (in)directly identify individuals. Thus, the information constitutes personal data in the sense of the Data Protection Directive[567] and the GDPR[568] (chapter 7, section 2.2.1) Moreover, the information contained in the data can be sensitive, reveal details about one's private life, or else flow from personal communications, falling in the remit of the right to respect for private and family life.

Protection of (any) data, as well as the information system where they reside, is expressed in terms of the classical canons of information security, applied to stored or transmitted data or the related services offered by or accessible via a network and information system: i) availability (services are operational as expected); ii) authenticity (users' claimed identity can

---

'bricks' of the universe. Information always concerns the physical world, and the world is always made sense of through information. The link with physics means that information can always be measured. The most basic measure is that created by Shannon, the bit, whereby 1 means 'no' and 0 means 'yes', which enables endless combinations that can describe anything, and lead to progressive simplification (or solutions) by reducing problems (questions) to the most elemental notions of yes/no.

[563] Tanenbaum and Wetherall (2011), chapters 1 and 2.

[564] David Isenberg, 'The Dawn of the 'Stupid Network'' (1998) 2 netWorker 24. Quoted in Van Schewick (2010), p. 108.

[565] Van Schewick (2010).

[566] As defined in the E-privacy Directive (2002/58/EC).

[567] 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 (Data Protection Directive) OJ L 281.

[568] General Data Protection Regulation (2016/679/EU).

be established); iii) integrity (transmitted/stored data are unchanged and complete); and iv) confidentiality (unauthorized parties cannot intercept communications/read stored data) (see chapters 4 and 5, section 3.2). The preservation of such canons is the objective of security management, which is based on risk management/assessment consisting in assessing the risk, or probability, that a threat will exploit an existing vulnerability in one's information system. The preservations of such canons is typically achieved through the repetition of a cycle composed of technical and organizational measures,[569] which aims to prevent-detect-minimize (as opposed to apprehend-punish). Loss of security is the opposite of security canons (as I discuss further in chapters 4 and 5). This also matters for network security. In traditional settings, user traffic is transmitted on a separate network to management traffic (e.g. configuration, performance and security management functions), called the telecommunication management network (TMN). "Network security management deals with setting up a secure management network as well as managing the security of information related to the three security planes of the ITU-T X.805 security architecture."[570] This changes with the introduction of next generation networks (NGNs), where the two types of traffic can be combined, so that threats affecting end-user traffic (i.e. information) could spill over to management traffic.

The applicable instruments concerning information security (*infra* section 3, chapter 4, section 1) require adopting organizational measures and technical tools to block the transmission or dissemination packets before information security canons are jeopardized. In this sense, they are preventative: if packets do not infect (terminal) equipment, the threat is avoided. The seminal judgment of the *Bundesverfassungsgericht*[571] made the interconnection between computing and privacy rights explicit, when it declared unconstitutional a North-Rhine Westphalia law allowing the domestic intelligence services to secretly search online private computers, to the effect of recognizing that confidentiality and integrity of information technology systems (computers, networks and other IT systems) form part of the tenets of

[569] Clarke identifies the following: scope definition, threat assessment, vulnerability assessment, risk assessment, risk management strategy and security plan and security audit. Roger Clarke, 'Introduction to Information Security' (*www.rogerclarke.com*, 2001) accessed 1 September 2016.
[570] International Telecommunication Union, *Security in Telecommunications and Information Technology. An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications* (ITU, Geneva, 2015), p. 65.
[571] Bundesverfassungsgericht (2008),1 BvR 2074/05 and 1 BvR 1254/07.

data protection (derived from articles 1(1) and 2(1) of the German Basic Law), adding to informational self-determination (chapter 2, section 3.3.2.1).[572]

***

Seen from this perspective, the effects of trading-off security with privacy rights online transcend the limits of count-terrorism and policing to acquire a completely different dimension. To what extent does the absence of cybercrime equate with cybersecurity, and the presence of cybersecurity with privacy rights? An abstract discussion does not prove conclusive. The relationship between security and privacy rights online must be looked at in the concrete, taking into account the complexity of cybersecurity, and of criminal activity taking place online. This calls for the methodological challenge. Before this, however, I look at the Union policy documents on cybersecurity, so as to define the scope of my enquiry.

2 UNION POLICY: A LA CARTE RECONCILIATION?

In this section I sketch the Union's policy concerning security in cyberspace, which has evolved in line with the expansion of its competences beyond the internal market.[573] I do so from the perspective of its interaction with policies on privacy rights with two objectives in mind. The first is expounding whether the policy documents support a normative reconciliation between cybersecurity and privacy rights. The approach could be seen as changing from an open acknowledgment of the complementarity between privacy rights, cybercrime prevention and network and information security (sections 2.2 and 2.3.1), to a more cautious approach (sections 2.3.2 and 2.3.3). If proposals always clarify the need to respect fundamental rights, reference to privacy rights seems to vary depending on the area of

[572]The decision extends the protection of personal data enshrined in article 10 of the German Basic Law "to ways of processing, which, in a narrower interpretation, do not fall under telecommunications, in particular to the contents of computer-hard disks and the use of Internet services. The new basic right supports the right to informational self-determination and thus takes the new risks into account, which the increasing networking of IT-systems involves." Press release of the judgment: http://www.bfdi.bund.de/cln_007/nn_672850/EN/PublicRelations/PressReleases/2008/07-08-OnlineSearches.html%3E. Werner Hülsmann, Kristina Irion and Cédric Laurant, 'Germany' in Privacy International (ed), *Global Surveillance Monitor* (2011).

[573] European Commission, *White Paper on Growth, Competitiveness, Employment. The Challenges and Ways forward into the 21st Century* ((Communication) COM (93) 700, 1993); Bangemann and al. (1994).

action tackled, which suggests different understandings of cyberspace. Hence, and secondly, since the analysis proves (perhaps unsurprisingly) non-conclusive, it calls urgently for the methodological challenge and sets its scope.

2.2 THE COMMISSION'S EARLY APPROACH

I begin by summarizing[574] the Commission's first approach as a way of highlighting policy changes over time. In 2000, the Commission issued a communication concerning cybercrime and the security of information infrastructure (network and information security and critical information infrastructure protection, viz. CIIP).[575] There, in relation to the latter, the Commission urged the adoption of a 'security by design' approach, and acknowledged 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."[576] As for cybercrime, it encouraged investing in prevention, as opposed to taking a traditional criminal law stance based on reaction:

> *"There is a need for effective substantive and procedural law instruments approximated at global, or at least at European level, to protect the victims of computer-related crime and to bring the perpetrators to justice. At the same time, personal communications, privacy and data protection, access to and dissemination of information, are fundamental rights in modern democracies. This is why the availability and use of effective prevention measures are desirable so as to reduce the need to apply enforcement measures. Any legislative measures that might be necessary to tackle computer-related crime need to strike the right balance between these important interests."*[577]

The communication also touched upon non-legislative measures, particularly on encryption, i.e. "an essential tool to facilitate the implementation and adoption of new

[574] I provided a comprehensive overview of the Union's approach towards cybersecurity from 1993 until 2012 in Maria Grazia Porcedda, *Data Protection and the Prevention of Cybercrime: the EU as an Area of Security?* (European University Institute Working Paper, Law 2012/25, 2012). A later work that analyses the policy from a political science background is by Christou (2015).
[575] European Commission, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime* ((Communication) COM (2000) 890 final, 2000).
[576] Ibid, p. 11.
[577] Ibid, p. 14.

services, including electronic commerce, and [that] can make a substantial contribution to the prevention of crime on the Internet."[578]

Shortly after, the Commission adopted a communication on network and information security (hereafter NIS),[579] understood as "the ability of a network[580] 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."[581] The document strikes the contemporary reader for its continued relevance and accuracy. Therein, the Commission proposed its 'three-pronged approach', exemplified in the figure below:

> *"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."*[582]

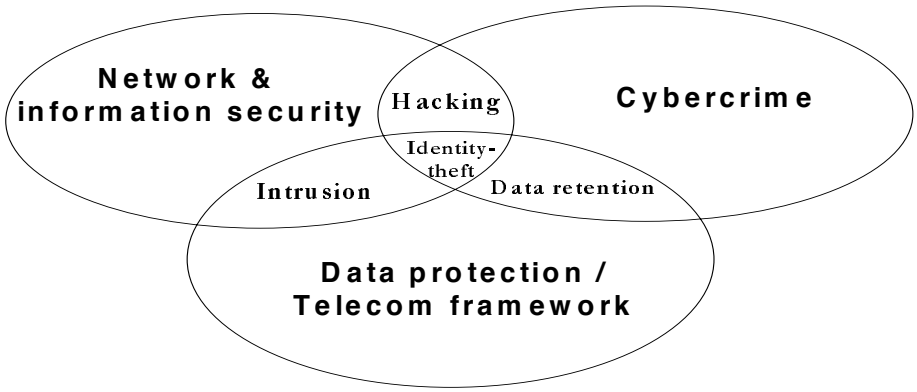


Figure 1 The Three-pronged approach, COM (2001) 298, p. 3

Accordingly, the protection of personal data, network and information security (NIS) and the prevention of cybercrime are seen as different aspects of the same phenomenon

[578] Ibid, p. 24.
[579] European Commission, *Network and Information Security: Proposal for a European Policy Approach* ((Communication) COM (2001) 298, 2001).
[580] Networks are defined 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 an 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.)." Ibid.
[581] Ibid, p. 3.
[582] Ibid.

(ensuring a safe development of the information society), which complement one another. Therefore, not only it is acknowledged that the "protection of privacy is a key policy objective in the European Union",[583] but also that privacy rights are not at odds with cyber-security and cybercrime prevention. The provisions contained in the data protection legal regime (i.e. article 17 of Directive 95/46/EC and articles 4-5 of then Directive 97/66/EC) were explicitly linked to the prevention of certain types of cybercrimes, and the safeguarding of network and information security. Furthermore, while acknowledging the need to conduct law enforcement cybercrime investigations, the communication stated that "these legal concerns should not create solutions where legal requirements lead to weakening the security of communication and information systems."[584] This clearly refers to encryption.

Later documents followed the established blueprint,[585] until a tipping point in mid 2000. Whether resulting from cyber-attacks suffered by Estonia (and then Georgia), or else the approach developed in the US,[586] the Commission and the Council seemed to endorse a 'national security' approach towards cyber-attacks, and cybercrimes in general, which are presented as existential threats to the nation and the Union.[587] In other words, the issue seems to have been securitized (chapter 2, section 1),[588] and greater importance attached to traditional crimes committed by electronic means, where reactive and forensic measures play a greater role.

[583] Ibid, p. 24.
[584] Ibid, p. 25.
[585] Porcedda (2012), *Data Protection and the Prevention of Cybercrime: the EU as an Area of Security?*
[586] Nissenbaum (2007), 'When Computer Security meets National Security'; Jerry Brito and Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy* (George Mason University 2011) < http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy>.
[587] European Council, *Report on the Implementation of the European Security Strategy – Providing Security in a Changing World* ((European Security Strategy) S407/08, 2008); Council, *The Stockholm Programme. An Open and Secure Europe Serving and Protecting Citizens, OJ C 115* (2010); European Commission (2010), *COM (2010) 171 final*.
[588] Nissenbaum (2007), 'When Computer Security meets National Security'; Dunn Cavelty (2013); Porcedda (2012), *Data Protection and the Prevention of Cybercrime: the EU as an Area of Security?*

2.3 THE 2013 CYBERSECURITY POLICY

In 2013 the European Commission jointly with the High Representative for Foreign Affairs and Security Policy adopted its first cybersecurity policy.[589] Therein, cybersecurity refers to

> *"the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."*[590]

Whereas the last sentence recalls the definition of NIS provided in the 2001 communication, the policy clarifies that cybersecurity is composed of three pillars: network and information security, law enforcement to tackle cybercrime, and defence, with their respective responsible actors (directorate generals and agencies) and regulatory regimes. Figure 2 below exemplifies the pillar structure.

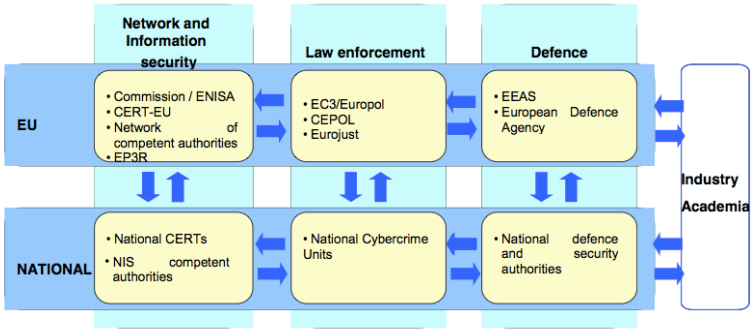


Figure 2 The integration between NIS, LEAs and defence[591]

If one compares the three pillars of the cybersecurity policy with the three prongs of the early policy documents (in figure 1 above), the first impression is that 'defence' has taken the place of the data protection/telecom framework, which would warrant a *prima facie* corroboration of the securitization hypothesis. Moreover, cybersecurity is depicted as a 'domain' with military relevance. Furthermore, the policy contains references to personal data as a right to safeguard, as well as to rules of its regulatory framework that have an import for NIS, but without stressing any further connections.

[589] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy (2013).
[590] Ibid, p. 3.
[591] Ibid, 17.

A broader reading of subsequent policy documents reveals a more nuanced, yet by no means straightforward, approach to the role of privacy rights.

2.3.1 NETWORK AND INFORMATION SECURITY (NIS)

Complementarity is clearly maintained in policy documents addressing NIS, which could be said to have assimilated the data protection/telecom framework prong, perhaps also owing to the common legal bases of the instruments adopted in this area (*infra*, section 3.2). Some months after the publication of the cybersecurity policy, the then DG Justice Commissioner Reding gave a speech[592] in front of the NATO Parliamentary Assembly where she depicted data protection rules and cybersecurity as two sides of the same coin. On the one hand, she said they serve the same purposes: preserving values online as they are offline and developing a single digital market. On the other hand, she noted they are mutually reinforcing: data minimization (chapter 7, section 3.2.4) reduces the damage of a successful cyber-attack, whereas better rules on personal data and 'cyber' increase trust and encourage people to use e-services. The tension between protecting rights and fighting crime would be solved by implementing good laws, such as mutual legal assistance treaties and data protection for police and judicial cooperation. The recent communication on cyber resilience, for instance, claims "making the EU a leading player in this field needs to be supported by a strong culture of data security, including for personal data, and an effective response to incidents."[593] The communication builds on the Digital Single Market Strategy,[594] where privacy rights are an integral component of trust and security (action 4 of the pillar "creating the right conditions and a level playing field to enable digital networks and innovative services to flourish"). The communication on cyber resilience envisages a single cyber market based on certification, which takes into account the rules contained in the GDPR, and in general for investment in cybersecurity. The multi-stakeholder approach enabled by the c-PPP (PPP in cybersecurity)

[592] Viviane Reding, *The EU's data protection rules and cyber security strategy: two sides of the same coin. Speech before the NATO Parliamentary Assembly/Luxembourg, SPEECH/13/436* (2013).
[593] European Commission, *Strengthening Europe's Cyber Resilience System* ((Communication) COM(2016) 640 final, 2016), p. 2.
[594] European Commission (2015), *COM (2015) 192 final*.

should be conducive to the definition of "common digital security, privacy and data protection requirements."[595]

2.3.2 CYBERCRIME

The cybersecurity policy refers to cybercrime as

> *"a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)."*[596]

Here, the Commission does not suggest different approaches depending on the type of crime, but rather refers to improving operational capabilities and coordination to fight against crimes with a cross-border dimension as diverse as child pornography, botnets and hacking. This includes the encouragement to ratify the Budapest Convention (see *infra*, section 3.3). Cybercrime was the object of several recent communications, including the Agenda on Security[597] and the Renewed European Internal Security Strategy (ISS),[598] where the approach depends on the matter at stake. The first line of defence against cybercrime, one of the three priorities of the Agenda on Security, is cybersecurity. To fight against cybercrime, the Commission sees it necessary to involve the whole supply-chain. Cooperation with the private sector is considered important also to address gaps in the fight against hate speech online and terrorist propaganda. To this effect, the Commission has launched an EU-level forum, where it also seeks to address concerns on encryption.[599] The creation of a European Forensic Area is a transversal pillar of the Agenda, to harmonize approaches concerning the quality of evidence and enhance its admissibility, which is seen as particularly relevant to support the

[595] European Commission (2016), *COM(2016) 640 final*, p. 12.
[596] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy (2013), p. 3.
[597] European Commission (2015), *The European Agenda on Security, COM(2015) 185 final*.
[598] Council, *Draft Annex Conclusions on the Renewed European Internal Security Strategy 2015-2020, 9797/15* (2015).
[599] European Digital Rights (EDRI), *What Digital Rights Are at Imminent Risk? All of Them* (EDRi-gram newsletter 14.17 2016).

fight against terrorism and organized crime. The Agenda contains no references to the interaction between privacy rights and cybercrime, let alone forensics. As for the Renewed ISS, measure 37 concerns discussing legal gaps in the fight against cybercrime and practical responses, particularly on encryption, IP addresses, cloud, jurisdiction, crypto-currencies, admissibility of e-evidence, PPPs and access to information. While the Renewed ISS emphasises the crucial importance in "ensuring full compliance with fundamental rights, including those relating to privacy, personal data protection and confidentiality of communications,[600] the text does not address the interaction between privacy rights, cybercrime and e-evidence. It explicitly calls for better information sharing, accessibility and interoperability to fight cybercrime, prevent and fight cybercrime as well as calling for safer and more secure ICTs to increase cybersecurity.

2.3.3 CYBER DEFENCE

Finally, following calls contained in the cybersecurity policy, the Council adopted its first policy on cyber defence in 2014.[601] Military approaches have become increasingly common, with cyberspace being referred to as the 5th domain of military activity. Unsurprisingly, the policy contains no references to privacy rights (or any other rights). The policy's main focus is developing capabilities in the area, particularly in terms of preparedness, detection and response, and to protect the CSDP communication networks, by means of developing an independent IT capacity for the EEAS. Hence the policy flirts with both law enforcement (development of forensics) and NIS (protection of own network), a link further developed in the Joint communication on hybrid threats.[602] There, cyber-attacks are seen as vectors for hybrid threats, which could be avoided thanks to improved NIS. Moreover, the cyber defence policy acknowledges the role of the private sector as the driver in the area and, given the dual-use nature of technology in the field, encourages civil-military cooperation to develop "strong technological capacities in Europe to mitigate threats and vulnerabilities",[603] e.g. on

[600] Council (2015), *Draft Annex Conclusions on the Renewed European ISS 2015-2020*, p. 4.
[601] Council, *EU Cyber Defence Policy Framework, 15585/14* (2014).
[602] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, *Joint Framework on countering hybrid threats. A European Union response* ((Joined communication) JOIN (2016) 18 final, 2016). There, hybrid threats are acts below the threshold of declared warfare that exploit the vulnerabilities of partners to achieve strategic objectives.
[603] Council (2014), *EU Cyber Defence Policy Framework*, p. 9.

cryptography, malware detection and NIS. The policy is silent as to the matter of exceptional access discussed in the introduction to this thesis.[604]

As it currently stands, none of the documents mentioned fall in the pure 'security v. privacy' category, but contain a number of ambiguities. Whenever the discussion touches upon NIS, the link with privacy rights is acknowledged, whereas it is ambiguous in discussions on cybercrime, and non-existent in the area of defence (much like other rights). Privacy rights are similarly absent in discussions on critical information infrastructure (CII) protection,[605] which links transversally the three areas. Such ambiguities stand in the way of providing an answer as to whether it is possible to reconcile security and privacy rights in the Union. What is needed is comprehension of the elements at stake, which are the object of the methodological challenge, to which I turn next.

3 THE METHODOLOGICAL CHALLENGE APPLIED TO CYBERSECURITY

The normative challenge must be complemented with the (jurisdiction-specific) methodological critique to the trade-off model I developed in chapter 2, based on three interrelated questions. First, what is being opposed? Second, are security and privacy the only relevant dimensions to be taken into account? And third, would giving up privacy be the most efficient solution, and why?

In this chapter I focus on the first question. Since the meaning of privacy rights was amply discussed in chapter 2 (section 3.3), here I concentrate on the meanings of 'cybersecurity' and add legal-descriptive value to them. The notions of cybersecurity on which I focus are those identified in the Union policy, namely network and information security (section 3.2) and cybercrime (section 3.3). Cyber-defence is, instead, beyond the scope of this research. Security is thus 'reworked' to signify the expression of the absence of threats codified in

[604] Abelson and others (2015).
[605] European Commission, *Critical information infrastructure protection. Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience* ((Communication) COM (2009) 149 final, 2009).

offences, and any reference to security in a given discussion of the 'trade-off' must be replaced by the specific offence under analysis (sections 3.2.1- 3.2.3 and sections 3.3.1-3.3.5). Section 3.3.6 focuses in particular on the uncertain notion of cybercrime.

3.1 CYBERSECURITY IN UNION LAW

The inherently political nature of cyberspace discussed *supra* (section 1.2) entails that the understanding of cybersecurity varies according to how broadly or narrowly cyberspace is construed (security of cyberspace or in cyberspace), as well as to what notion of 'security' is favoured (see chapter 2, section 1).[606] The fact that "cyberspace is flat, has no centre, is interconnected and worldwide, and classical territorial measures cannot be used"[607] has hindered legal consensus on the subject matter. This has especially proved the case since national security circles began laying eyes on the area,[608] and, as argued by Dunn Cavelty[609] (and Nissenbaum[610]), claimed a role that has been legitimized through securitizing discourses.

The United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security issued a report[611] suggesting the UN Charter should apply in cyberspace, and containing recommendations on a consensus of norms, rules, principles and confidence-building measures to address issues arising from the use of ICTs by states.[612] Certainly, a definition of

[606] In the political science literature, Christou looked at security as resilience, which can convey three different understandings. Christou (2015).
[607] Mattioli (2014), p. 27.
[608] In what is an ironic return to its origins, given that the creation of the Internet was funded by the US military research department, DARPA, to create a robust communication system able to back up the failure of the telephone system after a severe shock, e.g. a nuclear attack. Katie Hafner and Matthew Lyon, *Where Wizards Stay up Late. The Origins of the Internet* (Free Press (pocket books) 2003).
[609] Dunn Cavelty (2013).
[610] The securitization of cybersecurity was convincingly argued by Helen Nissenbaum and Lene Hansen, 'Digital Disaster, Cyber Security, and the Copenhagen School' (2009) 53 International Studies Quarterly 1155. It was later discussed in Samantha Adams and others, *The Governance of Cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK* (Tilburg University, 2015). I covered the subject in Porcedda (2012), 'Reviving Privacy: the Opportunity of Cybersecurity'.
[611] United Nations, General Assembly, *Report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174* (2015).
[612] Further work in the area can be followed at: United Nations, Office for Disarmament Affairs, 'Developments in the Field of Information and Telecommunications in the Context of International Security' <https://www.un.org/disarmament/topics/informationsecurity/> accessed 26 September 2016. Although this could favour state conduct based on *opinio iuris*, behaviour stemming from *opinio necessitatis* seems to be moulding rules.

cybersecurity is not in sight and, in fact, it may not be, as the term lends itself more to policy uses.[613] The most helpful insight may be that of the Venice Commission, which referred to cybersecurity as 'defensive', as opposed to SIGINT which is 'offensive'.[614] In its Agenda on Cybersecurity, the ITU shunned strict definitions in favour of the identification of pillars of action.[615]

Union law is no different. The term features mainly in policy documents, such as the 2013 joint communication discussed *supra* (section 2.3), where cybersecurity means "the safeguards and actions that can be used to protect the cyber domain…from those threats that are associated with or that may harm its interdependent networks and information infrastructure."[616] As noted above, the definition uses the expression 'domain', which bears closer resemblance to military language (e.g. cyber as the 5th domain), than expressions such as 'domain name' (*infra*, section 3.2), and at most could be understood as the sum of the sub-domains making up the Internet.[617] The definition, which is not free from criticism,[618] embodies a narrow version of cybersecurity (and cyberspace), in that it refers to generic threats to networks and information infrastructure, in this respect recalling the OECD security guidelines;[619] it is not concerned with human conduct in cyberspace at large, nor with crime related to content.[620]

This stands in contrast with the three pillars of cybersecurity enshrined in the policy, where 'cybercrime' seems to embrace all misconduct in cyberspace, thus appearing as a broader concept (*infra*, section 3.3). In the following sections I will tackle in turn two of the three pillars of the Union cybersecurity policy: network and information security, and cybercrime.

---

[613] The notion of cybersecurity could in fact include all of the following: computer security, information security, ICT security, network security, and infrastructure protection. Adams and others (2015), pp. 19-22. They also provide a definition at p. 26.
[614] Council of Europe (2015).
[615] International Telecommunications Union (ITU), 'Global Cybersecurity Agenda (GCA)' <http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx> accessed 26 September 2016. The five points are: 1. Legal Measures, 2. Technical and Procedural Measures. 3. Organizational Structures. 4. Capacity Building and 5. International Cooperation.
[616] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy (2013), *Cyber Security Strategy, JOIN (2013) 01 final*, p. 3.
[617] Markatos and Balzarotti (2013).
[618] For Mattioli, the EU policy should include "a human and information systems component, the underlying interconnection, and the aim to preserve the availability, integrity, authentication and confidentiality and non-repudiation" Mattioli (2014), p. 26.
[619] Organization for Economic Cooperation and Development (OECD), *Recommendation on Guidelines for the Security of Information and Networks. Towards a Culture of Secuirty* (2002). I discussed these and their relationship to EU law in Porcedda (2012), *Data Protection and the Prevention of Cybercrime: the EU as an Area of Security?*.
[620] I agree with such a distinction, as I discuss in chapter 4 and in previous work of mine cited in this chapter. A neat distinction between cybersecurity and cybersafety is also traced by Adams and others (2015), p. 26.

3.2 PILLAR 1: NETWORK AND INFORMATION SECURITY

After three years of debate, the Parliament and Council adopted the NIS Directive. Far from being a comprehensive text, the Directive has to adapt instead to an ecosystem of other legal instruments addressing different aspects of NIS. One such instruments is the Telecom Package, particularly the e-Privacy and Framework Directives,[621] both of which are set to be overhauled: the Commission proposed a Directive setting up an electronic commerce code and recasting of the telecom framework,[622] and has announced it will present a revised version of the e-privacy directive by the end of 2016 so as to address its non-applicability to information society services. Another is the eIDAs Regulation concerning e-identity and trust services.[623] The last is the Regulation setting up ENISA.[624]

The current outlook has to do with the development of the regulatory framework reflecting the evolution of the field since states liberalised telecommunications,[625] as well as of EU competences. Software was addressed instead from a copyright perspective. Public networks and connectivity services (public electronic communications networks and publicly available electronic communication services), mostly offered by traditional telecommunications companies, were regulated separately from services available online, which at the time constituted a separate fraction of the market (information society services, e-commerce and audio-visual services). E-Privacy rights were addressed in relation to the former, not the latter. Security issues were regulated as factors of competition and enablers of rights. Providers of private networks, and economic actors enabling connectivity but not owning the network,

[621] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive), OJ L 108, as amended by Directive 2009/140/EC of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, OJ L 337.

[622] European Commission, *Proposal for a Directive Establishing the European Electronic Communications Code* ((Communication) COM(2016) 590 final, 2016/0288 (COD), 2016). The repeal of the e-Privacy Directive is contained in the Digital Single Market Strategy, the GDPR, and has been recently reaffirmed by DG Connect: https://ec.europa.eu/digital-single-market/en/online-privacy.

[623] Regulation 910/2014/EU of the European Parliament and Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, OJ L257.

[624] Regulation 526/2013/EU of the European Parliament and the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004.

[625] For an excellent overview, see Ian Walden (ed), *Telecommunications Law and Regulation (4th edition)* (Oxford University Press 2012); Lilian Edwards and Charlotte Waelde, *Law and the Internet* (Hart Publishing 2009).

were not concerned by EU law; no specific legislation existed for actors offering ICT-specific security.

The instruments explicitly addressing NIS stem from such convoluted development, and share the same legal basis: approximation of law, currently article 114 TFEU (previously article 95 TEC).[626] In this respect, it could be said that NIS is primarily oriented towards the Internal market, rather than the AFJS; indeed, the responsible DG in the area of NIS is DG Connect. Such panoply of overlapping instruments risks engendering a regulatory cacophony. Although the instruments insist on the validity of definitions solely within the scope of their remit, there seems to be convergence on the understanding of 'networks' and 'information systems'.

As for networks, the NIS Directive refers to the Framework Directive, which defines networks as

NIS Directive, art 4 (1) (a)	**Framework Directive, art. 2 (a)**
An electronic communications network within the meaning of point (a) of Article 2 of the Framework Directive	'Electronic communications network' means transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed
Recital 7: not public	Art. 2 (d) 'public communications network' means an electronic communications network used wholly or mainly for the provision of electronic communications services available to the public which support the transfer of information between network termination points

Table 1 Definition of networks

[626] According to Savin, the rationale for basing several internet-related instruments on article 114 TFEU is the fear that the lack of harmonization may impinge on the development of the single digital market, rather than unruly development. Andrej Savin, *EU Internet Law* (Elgar 2013).

Information systems, in the context of NIS, are only defined in art. 4 (1) (b) of the NIS Directive as "any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data." Alternatively, information systems are also to be understood as "(c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance." The definition underlines the interrelatedness, and almost indivisibility, between network and information systems, in that there is a mutually vital relationship between the two.

Security of network and information systems/network and information security are defined in the relevant instruments as follows:

ENISA Regulation, art. 1(3):	**NIS Directive, art. 4 (2)**	**Proposed electronic communication code, art. 2 (22)**	**eIDAS Regulation, rec. 44, 48 and 72**
'Network and information security' means	'Security of network and information systems' means	'Security' of networks and services means:	A high level of security
the ability of a network or an information system to resist, at a given level of confidence, **accidental** events or **unlawful** or **malicious** actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via those networks and systems.	the ability of network and information systems to resist, at a given level of confidence, **any action** that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or **processed** data or the related services offered by, or accessible via, those network and information systems.	the ability of **electronic communications networks and services** to resist, at a given level of confidence, **any** **action** that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those networks or services.	undefined
Events: Natural and man-made	Only man-made	Only man-made	
Data: stored or transmitted	Data: stored or transmitted or processed	Data: stored or transmitted or processed	

Table 2 Definition of information security

The differences between the definitions concern the following: the scope of threats to security, which may include natural disasters (ENISA's definition); the scope of data which can include further operations on top of transmission and storage (NIS and Framework Directive); and the explicit ambit of application. The latter harbours the most visible differences, which I briefly elucidate in the following.

3.2.1 SCOPE OF THE NIS DIRECTIVE

The establishment of security and notification requirements mandated by the NIS Directive (art. 1 (d))[627] concerns operators of essential services and digital service providers.

Operators of essential services are public or private entities which meet three cumulative criteria (arts. 4 (4) and 5 (1)): the service is 'essential for the maintenance of critical societal and/or economic activities', its provision 'depends on network and information systems' and would be highly disrupted by 'an incident', meaning "any event having an actual adverse effect" (art. 4 (7)). Its Annex II specifies the types of operators of essential services, which concern the wide sectors of energy, transport, banking, financial market infrastructures, health sector, the drinking water supply and distribution, and the digital infrastructure. The latter includes internet exchange points (IXPs), domain name system (DNS) service providers[628] and Top Level Domain name registries, which can be defined as CII. In this respect, the NIS Directive seems to fulfil an important CIIP function, though the instrument clarifies that it does not prejudice the identification of critical infrastructures at large, which is the objective of Directive 2008/141[629] instead.

[627] It should be noted that the other objectives of the NIS Directive are not of immediate relevance for this chapter (and, in general, this thesis).
[628] Defined in article 4 as follows: (13) 'internet exchange point (IXP)' means a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic; (14) 'domain name system (DNS)' means a hierarchical distributed naming system in a network which refers queries for domain names; (15) 'DNS service provider' means an entity which provides DNS services on the internet.
[629] Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection, OJ L 345.

Digital services (art. 4 (5)) are one of the following three types of information society services: search engines, online marketplaces and cloud computing.[630] Information society services are "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request."[631]

The approach proposed by the Directive is that of resistance, i.e. the logic of prevent-detect-minimize incidents described *supra* (section 1.2.2), as exemplified by the logic of risk management/assessment and handling which permeates the text, and the provisions in article 14 (2) and (6) on operators of essential services and article 16 (2) and (7) on digital services.

3.2.2 SCOPE OF THE ELECTRONIC COMMUNICATIONS FRAMEWORK

As noted above, the electronic communications framework applies to (public) electronic communication networks and the elements thereof, which can also be the object of more specific legislation (e.g. the case of satellites). The purpose of such public networks is to mainly, if not wholly, provide electronic communications services "available to the public which support the transfer of information between network termination points." Pursuant to art. 2 (c) of the Framework Directive, an 'electronic communications service' is "a service

[630] According to the NIS directive, (17) 'online marketplace' means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council (1) to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace; (18) 'online search engine' means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found; (19) 'cloud computing service' means a digital service that enables access to a scalable and elastic pool of shareable computing resources.

[631] Art. 1 (b) of Directive 2015/1535/EU of the European Parliament and of the Council of 9 September 2015 Laying down a Procedure for the Provision of Information in the Field of Technical Regulations and of Rules on Information Society services (codification), OJ L 241.

normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services…which do not consist wholly or mainly in the conveyance of signals on electronic communications networks." The proposed electronic communication code clarifies that communications services such as "voice telephony, messaging services and electronic mail conveyance services are covered" (proposed recital 11).

3.2.3 THE EIDAS FRAMEWORK

The eIDAs Regulation concerns the security of e-identification services and of trust services.

Following article 3 (1), electronic identification means "the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person." Person identification data are "a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established" (art. 3 (3)).

A trust service is "an electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services." (art. 3 (16)).

The Regulation does not explicitly qualify the nature of the services as information society services (ISSs). It can be argued that eIDAS would not fall in the definition of ISS because they do not operate entirely by electronic means, in that they need a physical support (i.e. hardware) to work. Moreover, the combined purpose of the eIDAs Regulation is, in line with articles 1 and 4 ('internal market principle'), the free movement as well as 'an adequate level

of security' of e-ID and trust services. The latter is the main focus of the Regulation because, as clarified in the opening recitals, the uncertain level of security determined by the lack of a proper regulatory framework hampers the free circulation of such services (recitals 1 and 2).

It can be argued that e-ID and trust services are instead means of securing information systems in the sense of article 4 (1) (c) of the NIS Directive, "i.e. digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance" in that they oversee the authenticity and integrity "of stored or transmitted or **processed** data" (whether personal identity or documents) as defined by article 4 (2) of the NIS Directive.

***

Based on the analysis conducted above, I argue that the three instruments engender a similar idea of network and information security (either separately or jointly), which, it should be remembered, is preventative rather than reactionary, and falls in the remit of the internal market rather than the AFSJ. The instruments taken into account differ, in that they apply this notion of security to different elements of cyberspace. Following the blueprint developed in chapter 2, it is possible to reformulate the trade-off argument in the context of NIS (which will be reflected upon in chapter 4) as follows:

*value (V) protected by privacy rights v. measures to preserve the availability, authenticity, integrity or confidentiality of stored or transmitted or processed **data** or the related essential/digital services offered by, or accessible via network and information systems.*

*value (V) protected by privacy rights v. measures to preserve the availability, authenticity, integrity or confidentiality of stored or transmitted or processed **data** or the related communication services offered by, or accessible via network and information systems, and the network and information systems themselves.*

*value (V) protected by privacy rights v. measures to preserve authenticity and integrity of stored or transmitted or processed **data** offered by e-identification schemes and trust services, accessible via network and information systems."*

3.3 PILLAR 2: SECURITY AGAINST CYBERCRIME (CRIME ONLINE AND FORENSICS)

The adoption of rules specific to cyberspace is recent. At the beginning of the new millennium Brenner[632] questioned the empirical premise whereby cybercrimes represent a new legal phenomenon, since "they involve conduct that is committed wholly or partly in … the virtual world of cyberspace". While warning that the use of a new tool to commit crimes or their virtual character[633] may not justify, *per se*, the introduction of a new legal framework, she considered that "we must accept the possibility that unacceptable social harms can be inflicted inside cyberspace and act accordingly, if and when the need to do so arises". Brenner reasoned that the expanding importance of cyberspace may have presented, for example, the need to adopt specific rules to tackle the great harms that cyber-criminality can inflict (also due to the possible greater scale of misconduct), as a deterrent to such conduct, or the increased difficulty in investigating and apprehending criminals.[634] Moreover, these issues, which Flanagan calls of 'degree', interact with issues of 'kind', i.e. the appearance of new forms of misconduct and dual criminality issues.[635] All these challenges have materialized (section 1.2.1), and since then new kinds of misconduct have also appeared, leading to several dedicated legal instruments at the national and international level.[636]

The latter is the Cybercrime Convention[637] sponsored by the Council of Europe, spurred by the increased difficulty in investigating and apprehending criminals due to the intrinsically cross-jurisdictional character of cybercrimes.[638] The instrument, in fact, addresses the problem of dual criminality (whereby international judicial cooperation can take place only if a conduct is similarly criminalized in both countries), as well as the preservation, gathering and international exchange of evidence necessary to conduct investigations against cybercriminals. The instrument provides common definitions of cybercrimes falling into four

[632] Susan Brenner, 'Is There Such a Thing as 'Virtual Crime'?' (2001) 4 California Criminal Law Review. This goes in hand with Easterbrook's doubts about cyberlaw as 'the law of the horse'.
[633] Brenner noted that cybercrime is not the first instance of 'virtual crime'; notable (problematic) precedents in common law being the criminalization of certain thoughts and witchcraft.
[634] Brenner (2001).
[635] Anne Flanagan, 'The Law and Computer Crime: Reading the Script of Reform' (2005) 13 International Journal of Law and Information Technology 98.
[636] See, for instance, Susan Brenner and Bert-Jaap Koops (eds), *Cybercrime and Jurisdiction. A Global Survey* (TMC Asser Press 2006); Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (International Telecommunication Union, Geneva, 2012), chapters 5 and 6; Porcedda (2014), 'Rule of Law and Human Rights in Cyberspace'; United Nations (2013), chapter 3 and annex 3.
[637] Convention on Cybercrime, Council of Europe, CETS n. 105 23 November 2001.
[638] Explanatory Memorandum of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe. Susan Brenner, 'The Council of Europe's Convention' in Jack M. Balkin et al. (ed), *Cybercrime, Digital Cops in a Networked Environment* (New York University Press 2007); Flanagan (2005).

(according to Gercke, not wholly consistent) categories, leading to overlaps: "Three categories focus on the object of legal protection: "offences against the confidentiality, integrity and availability of computer data and systems; content-related offences; and copyright related offences". The fourth category of "computer-related offences" does not focus on the object of legal protection, but on the method used to commit the crime."[639]

The approach of Union law to harmful conduct in cyberspace reflects international developments and appears to be piecemeal (and, to some, ineffective[640]). Art. 83 TFEU enables the EU to establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis. One of these is 'computer crime'. According to Gercke computer crime (in general, not with reference to the Lisbon Treaty) refers to cybercrime 'in a narrow sense'[641] (narrow cybercrime, see chapter 4), i.e. conduct by means of computer systems and directed against them and the data they process.

Apart from Directive 2013/40, there is no comprehensive 'cybercrime' instrument. Moreover, the relationship shown in the policy documents between certain forms of cybercrime and cybersecurity is not replicated in laws addressing the specific crime. As a result, it does not seem possible to find a common denominator, as identified in the case of NIS. Since the Budapest Convention "is the legal framework of reference for combating cybercrime, including attacks against information systems" (Directive 2013/40/EU, recital 15), it seems apt to investigate 'cybercrimes' in Union law by reference to the categories of the Cybercrime Convention. For each I refine the understanding of crimes against CIA (section 3.3.1), computer-related crimes (section 3.3.2), content-related crime (section 3.3.3) and racism and xenophobia (section 3.3.4). I must stress that I purposefully do not include copyright infringement; although it is a very interesting case of lobbies pushing[642] for quasi-criminalization and greater monitoring (see chapter 4), it is not a criminal offence in EU law. An additional section covers crimes not yet listed in the Convention (section 3.3.5), whereas the final section contains reflections on the notion of cybercrime and the import of the Convention in Union law. Note that precisely defining the remit of each offence may be

[639] Gercke (2012), p. 12.
[640] Francesco Calderoni, 'The European Legal Framework on Cybercrime: Striving for an Effective Implementation' (2010) 54 Crime, Law and Social Change 339-357.
[641] Gercke (2012), p. 11.
[642] With reference to the UK, see Flanagan (2005).

difficult since, as the applicable law instruments recognize, a single offence may involve "several stages of a criminal act, where each stage alone could pose a serious risk to public interests" (recital 5 of Dir. 2013/40, with reference to botnets).

3.3.1 CIA CRIMES: DIRECTIVE ON ATTACKS AGAINST INFORMATION SYSTEMS

The Directive on attacks against information systems[643] was adopted pursuant to article 83 (1) TFEU, hence to "establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension". The Directive is thus solidly anchored in the AFSJ. While it repeals the previous Council Framework Decision 2005/222/JHA, the Directive maintains its original links with the Council of Europe Convention on Cybercrime (*infra*, section 3.3.6). The Directive refers openly to the notion of 'cybercrime', which is mentioned once in the main text (art. 17) and several times in the recitals.[644]

The idea of (cyber)security enshrined in the Directive is the protection against, and if possible prevention of, attacks against *any* information systems (the scope of the Directive is not limited by the ownership or purpose of information systems). An information system is "a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance". Computer data are "a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function." I will reason on the convergence between Directive 2013/40 and NIS in chapter 4.

The Directive identifies five categories of crimes against CIA, which correspond to the relevant categories of the Cybercrime Convention (articles 2-6), and which are to be criminalized when perpetrated without right, i.e. conduct "including access, interference, or

[643] Directive 2013/40/EU of the European Parliament and the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA, OJL 218.
[644] These are 2, 14, 15, 24, where NIS is also mentioned, 25, 26 where resilience of critical infrastructures is mentioned, and 28.

interception, which is not authorized by the owner or by another right holder of the system or of part of it, or not permitted under national law." (art. 2 (d)). They are defined as follows.

First, illegal access to information systems (art. 3): "when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor." This provision covers hacking, cracking and abuse of credentials.

Second, illegal system interference (art. 4): "seriously hindering or interrupting the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor." This includes the creation of botnets (i.e. robot networks), viz. "the act of establishing remote control over a significant number of computers by infecting them with malicious software through targeted cyber attacks. Once created, the infected network of computers that constitute the botnet can be activated without the computer users' knowledge in order to launch a large-scale cyber attack, which usually has the capacity to cause serious damage" (recital 5). The large-scale attack is typically (distributed) denial of service attacks, whereby the enslaved computers, called zombies, send more access requests to a server than it can handle with the purpose of paralyzing it. A recent attack of this kind was launched against the website Krebs on Security.[645] Note that a DDoS affects availability and integrity without gaining confidential information concerning users.[646] In my opinion, if spamming (i.e. sending SMTP traffic to port 25) has the objective of flooding an email account, it would be akin to a denial of service attack and qualify as illegal system interference. Botnets can also be used to distribute illicit content, as is the case of fast-flux networks,[647] i.e. networks whose zombie components change constantly and quickly (so that take-down of some does not affect the operation of the rest of the network).

Third, illegal data interference (art 5): "deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and without right, is punishable as a criminal offence, at least for cases which

[645] John Naughton, 'Why the Internet of Things is the New Magic Ingredient for Cyber Criminals' *The Guardian* (2 October 2016).
[646] Konrad Rieck, 'Assisted Discovery of Vulnerabilities' (Third Summer School on Security and Privacy: "Building Trust in the Information Age", Cagliari, September 2014).
[647] Igino Corona, 'Machine-Learning Approaches to the Detection of Fast Flux Networks and PDF malware' (Third Summer School on Security and Privacy: "Building Trust in the Information Age", Cagliari, September 2014).

are not minor". This provision covers the case of worms, viruses and malware such as Trojans. Viruses are a string of code that self-propagates and needs a host environment; worms are self-contained programs that self-propagate (the modern versions act as mass scanners); malware, meaning malicious software, violates the security policy but does not self propagate.[648]

Fourth, illegal interception (art. 6): "intercepting, by technical means, non-public transmissions of computer data to, from, or within an information system, including electromagnetic emissions from an information system carrying such computer data, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor". Recital (9) clarifies that "Interception includes, but is not necessarily limited to, the listening to, monitoring or surveillance of the content of communications and the procuring of the content of data either directly, through access and use of the information systems, or indirectly through the use of electronic eavesdropping or tapping devices by technical means." Forms of illegal interception are unlawful probes and spyware (i.e. spying software), various forms of sniffers, such as keysniffing,[649] as well as copying data.[650] Honeypots, i.e. systems designed with flaws known to cyber-offenders, so as to attract them, may be seen as falling within this category.[651]

Fifth, tools used for committing offences (art 7): "the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence, at least for cases which are not minor: (a) a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6; (b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed." Recital (16) clarifies the wish not to carve in stone the tools used to commit cyber-attacks, including the creation of botnets, to factor in the diversity of attacks and the "rapid developments in hardware and software". Moreover, it clarifies that

[648] Stefano Zanero, 'Behavior-based Methods for Automated, Scalable Malware Analysis' (Third Summer School on Security and Privacy: "Building Trust in the Information Age", Cagliari, September 2014).
[649] Sandro Iannaccone, 'Cybersicurezza, Attenti alle Tastiere Wireless' *La Repubblica*.
[650] David Kravets, 'Internet Tracking Software Maker to Face Wiretapping Trial, Court Rules' *ArsTechnica.com* (17 August 2016).
[651] For a thorough comparative discussion, see Anne Flanagan and Ian Walden, 'Honeypots: a Sticky Legal Landscape?' (2009) 29 Rutgers Computer and Technology Law Journal 317.

the use of tools "to test the reliability of information technology products or the security of information systems", a.k.a. white hat hacking, should be allowed.

Article 8 also criminalizes incitement to, and aiding and abetting of, the crimes identified above.

The Directive does not criminalize identity theft, although article 9 (5) invites Member State to consider as an aggravating circumstance the commission of illegal data and system interference "by misusing the personal data of another person, with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner…unless those circumstances are already covered by another offence, punishable under national law." According to recital 14, "setting up effective measures against identity theft and other identity-related offences constitutes another important element of an integrated approach against cybercrime."

***

Based on the blueprint developed in chapter 2, the trade-off between privacy rights and (cyber)security in the context of attacks against information systems can be reformulated as the following relations (which will be discussed in chapter four):

"value (V) protected by privacy rights v. measures to counter access without right, to the whole or to any part of an information system, by infringing a security measure (Illegal access to information systems)"

"value (V) protected by privacy rights v. measures to counter seriously hindering or interrupting the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible (Illegal system interference)"

"value (V) protected by privacy rights v. measures to counter deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible (Illegal data interference)"

"value (V) protected by privacy rights v. measures to counter intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data (Illegal interception).

"value (V) protected by privacy rights v. measures to counter the use… of tools for committing offences."

3.3.2 COMPUTER-RELATED CRIMES

3.3.2.1 Fraud: Council Framework Decision 2001/413/JHA

Council Framework Decision 2001/413/JHA addresses fraud and counterfeiting of non-cash means of payment. It is based on article 34(2) (b) of the old TEU. The Commission plans to introduce a legislative proposal to update the instrument,[652] most likely under article 83.1 TFEU, which identifies counterfeiting of means of payment as a serious crime with a cross-border dimension.

The Decision identifies a number of offences against non-cash payment instruments, which are "a corporeal instrument, other than legal tender (bank notes and coins), enabling, by its specific nature…the holder or user to transfer money or monetary value, as for example credit cards, eurocheque cards, other cards issued by financial institutions…which is protected against imitation or fraudulent use, for example through design, coding or signature (article 1 (a)).

Since the Decision was adopted before the conclusion of the Budapest Convention, it does not contain a connection clause, although it generically refers to the work of the CoE in this area (recital 2). Hence, the text does not contain any legally meaningful references to cybercrimes. Nevertheless, the decision identifies two categories of offences related to the use of ICT.

Pursuant to article 3, it should be a criminal offence to intentionally perform or cause "a transfer of money or monetary value and thereby causing an unauthorised loss of property for another person, with the intention of procuring an unauthorised economic benefit for the person committing the offence or for a third party, by: without right introducing, altering, deleting or suppressing computer data, in particular *identification* data, or without right interfering with the functioning of a computer programme or system." An example is the case

[652] European Commission, *Delivering on the European Agenda on Security to Fight against Terrorism and Pave the Way towards an Effective and Genuine Security Union* ((Communication) COM (2016) 230 final, 2016).

of a criminal re-directing online banking users to a bogus banking website, or sending bogus emails (a.k.a. phishing), for harvesting their username and passwords, and then accessing the legitimate banking website with the stolen credentials to siphon money off the unfortunate person's bank account. Another example is cyber-extortion, whereby targets, which could be an online gambling site but also individual users, are infected and dispossessed of the control of their machine, unless they pay a ransom (a.k.a. ransomware). The Decision is silent about the definition of 'without right', though for the sake of consistent interpretation the definition provided in Dir. 2013/40/EC could also apply here.

Article 4 lays down two additional offences, when committed intentionally, namely "the fraudulent making, receiving, obtaining, sale or transfer to another person or possession of instruments, articles, computer programmes and any other means peculiarly adapted for the commission of" counterfeiting or falsification of a payment instrument in order for it to be used fraudulently (pursuant to Article 2(b)), or "computer programmes the purpose of which is the commission of any of the offences described under Article 3". In this respect, the offence contains an element of forgery (see below).

Recital (10) clarifies that the intention of the Decision is "to encourage operators to provide … protection to payment instruments issued by them, and thereby to add an element of prevention to the instrument." Such encouragement to the effect of adding an element of prevention has progressively become the object of specific legal obligations,[653] currently enshrined in the Directive on payment services in the internal market[654] (discussed in chapter 4).

***

Following the blueprint developed in chapter 2 and put in practice in previous subsections, the trade-off between privacy rights and (cyber)security in the context of fraud could be reformulated as follows:

"value (V) protected by privacy rights v. measures to counter the altering, deleting or suppressing of computer data, in particular identification data, or interfering with the

[653] The paucity of cyber security-related rules requiring to enforce prevention is noted by Adams and others (2015).
[654] Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337.

functioning of a computer programme or system, for the sake of procuring an unauthorised economic benefit for the person committing the offence" (art. 3) and

"value (V) protected by privacy rights v. countering the fraudulent making, receiving, obtaining, sale or transfer to another person or possession of instruments, articles, computer programmes and any other means peculiarly adapted for the commission of counterfeiting or falsifying of a payment instrument in order for it to be used fraudulently, or computer programmes the purpose of which is the commission of any of the offences described under Article 3."

3.3.2.2 Forgery: the eIDAS Regulation

Thus far, there are no specific instruments criminalizing forgery. Article 4 of Council Framework Decision 2001/413/JHA addresses forgery insofar as means of payment are concerned. On the other hand, the eIDAS Regulation (*supra*, section 3.2.3), contains measures aimed at the prevention of forgery as defined in the Cybercrime Convention (art. 7), i.e. the "input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible." I will come back to this in chapter 4.

3.3.3 CHILD PORNOGRAPHY: DIRECTIVE 2011/92

The Directive on combating child sexual abuse, exploitation and pornography[655] was adopted pursuant to two legal bases in the AFSJ. One is article 82(2) on minimum rules concerning criminal matters having a cross-border dimension, so as to facilitate mutual recognition of judgments and judicial decisions and police and judicial cooperation. The other is article 83(1) on establishing minimum rules and sanctions in the area of sexual exploitation of children, as a serious crime with a cross-border dimension.

[655] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing Council Framework Decision 2004/68/JHA, OJ L 335.

The Directive defines four categories of serious crime: offences concerning sexual abuse (article 3), offences concerning sexual exploitation (article 4), offences concerning child pornography (article 5) and solicitation of children for sexual purposes (article 6). Children are persons below 18 pursuant to article 2(a), though the Directive enables a degree of flexibility by taking into account the age of sexual consent, which varies depending on national law. Recognizing that the use of new technologies and the Internet is enabling the increase and spread of sexual abuse, exploitation and pornography of children (recital 3), articles 5 and 6 provide a specific reference to information and communication technologies. However, unlike Directive 2013/40, it contains no clauses of connection with the Cybercrime Convention (art. 9). Hence, unlike references contained in policy documents cited in this chapter, offences against children conducted by means of information technology are not legally classified as cybercrime in the EU legal order.

Article 5 defines offences concerning child pornography, which is defined broadly by article 2 (c) so as to include: any material, including realistic images,[656] visually depicting a child, or someone appearing to be a child, engaged in real or simulated explicit conduct; or any depiction, including realistic images, of the sexual organs of a child, or someone appearing to be a child, for primarily sexual purposes. Article 5 (3) criminalizes "Knowingly obtaining access, by means of information and communication technology, to child pornography" (which shall be punishable by a maximum term of imprisonment of at least 1 year). Moreover, article 25 lays down measures against websites containing or disseminating child pornography. In the words of recital 46, "making it more difficult for offenders to upload such content onto the publicly accessible web" (and conversely "seeking to secure the removal of such content from servers"), is seen as a necessary measure to combat child pornography, which "cannot be construed as the expression of an opinion". Pursuant to paragraph 1, Member States must adopt measures to ensure the "prompt removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory".

In the light of the fact that third countries may be unwilling or unable to cooperate (recital 47), paragraph 2 enables Member States to take measures to block access to web pages containing or disseminating child pornography towards the Internet users *within their territory*. Such measures could be based on various types of public action, such as legislative,

[656] This is the so-called pseudo pornography. See chapter 4 and Flanagan (2005).

non-legislative, judicial or other (recital 47), so long as they include adequate safeguards, respect the principles of necessity and proportionality, including the provision of information to interested parties, and enable judicial redress.

The Directive recognizes that the use of information and communication technology facilitates the online solicitation of children for sexual purposes via social networking websites and chat rooms (recital 12). Article 6 defines solicitation of children for sexual purposes broadly, and encompasses those offences identified in articles 3 and 5 when conducted intentionally and by means of information and communication technology. Hence, it is a crime if an adult proposes a child (who has not reached the age of sexual consent) to meet for the purposes of engaging in sexual activities (Article 3(4)), or else to produce child pornography (art. 5(6)), and "that proposal was followed by material acts leading to such a meeting." Pursuant to (the somewhat unclear) paragraph 2, the Directive mandates Member States to take the necessary measures to criminalize an adult who attempts, by means of information and communication technology, to acquire or possess child pornography (art. 5 (2)) or to engage in sexual abuse as defined in article 3, §2-6, for the sake of providing child pornography concerning the solicited child.

***

Following the blueprint developed in chapter two, it is possible to reformulate the trade-off argument as "privacy v. combating child exploitation, abuse and pornography by means of information and communication technology", and in particular the offences seen in articles 5 and 6.

As for article 6, the trade-off can be reformulated as "*value (V) of privacy rights v. measures to fight against the solicitation of children for sexual purposes*".

The fight against child pornography by means of information and communication technology was further specified by article 25, so as to become:

"value (V) protected by privacy rights v. removal of web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory" and

"value (V) protected by privacy rights v. blocking access to web pages containing or disseminating child pornography towards the Internet users within their territory".

3.3.4 RACISM AND XENOPHOBIA: FRAMEWORK DECISION 2008/933

Racism and xenophobia do not form part of the Cybercrime Convention, but rather are the subject of an additional protocol,[657] due to the resistance of some of its parties to include offences that could impinge upon freedom of expression. Those provisions include the case of cyber-bullying, trolling and cyber-stalking. The Council Framework Decision criminalizing racism and xenophobia[658] contains neither references to ICTs, nor connection clauses with the additional protocol to the Convention. Hence, it will not be taken into account in this study.

3.3.5 OTHER CRIMES WHERE E-DATA ARE EVIDENCE

In section 1.2.1 I referred to the fact that cyberspace can harbour evidence relevant for the fight against offences that do not fall within the (broad category of) cybercrime. Article 14 of the Budapest Convention recognizes these needs, to the extent that it enables parties to apply the same procedural rules applicable to offences contained in the Convention for the collection of electronic evidence relating to any criminal investigation. In EU law, references to measures for the collection of evidence relating to offences other than cybercrimes are found in the proposed Directive on counter-terrorism, and mentioned in passing (in a recital) in the Directive on human trafficking.

3.3.5.1 Counter-terrorism

The Council Framework Decision on combating terrorism[659] currently in force does not contain rules concerning 'cyber-terrorism', i.e. terrorism mediated by the use of information technologies, with the (mild) exception of article 1(1) (d), whereby "causing extensive destruction to … an infrastructure facility, including an information system" is a terrorist offence. This provision could be relied upon in case of large-scale cyber attacks.

[657] Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, Council of Europe, ETS n. 189.
[658] Council Framework Decision 2008/913/JHA of 28 November 2008 on Combating Certain Forms and Expressions of Racism and Xenophobia by Means of Criminal Law, OJ L 328. A discussion of this decision can be found in Fundamental Rights Agency, *Ensuring Justice for Hate Crime Victims: Professional Perspectives* (2016).
[659] Framework Decision 2008/919/JHA on Combatting Terrorism.

The text is currently being revised. The proposed Directive on combating terrorism[660] is based, like other post-Lisbon instruments analysed in this chapter, on articles 83(1) and 82(2) (c) TFEU, and it aims at updating the legal framework particularly to take into account "foreign terrorist fighters and terrorist financing". Recital 5 clarifies that "these forms of behaviour should be punishable also if committed through the Internet, including social media."

A proposal to introduce a provision on measures against websites publicly inciting the committing of a terrorist offence, in line with Article 25 of Directive 2011/92/EU discussed above, was instead transformed into a new paragraph in recital 7. It reads "To strengthen actions against public provocation to commit a terrorist offence, and also taking into account the rise of new technologies, it seems appropriate for Member States to envisage measures to remove or to block access to webpages publicly inciting to commit terrorist offences."

Finally, article 3 (2) (i) includes among terrorist offences "illegal system interference or illegal data interference, as referred to in Article 4 and Article 5 of Directive 2013/40/EU on attacks against information systems in cases where Article 9, paragraph (3) or (4)(b) and (c) of the said Directive apply", i.e. "where a significant number of information systems have been affected through the use of a tool, referred to in Article 7, designed or adapted primarily for that purpose" (art. 9 (3)); or where they cause serious damage (art. 9 (4) (b); or where they are committed against a critical infrastructure information system (art. 9 (4) (c))." The explanatory memorandum construes this as a reference to cyber attacks.

***

Hence, it is possible to reformulate the trade-off between security and privacy as follows

"value (V) protected by privacy rights v. measures to counter illegal system interference or illegal data interference where a significant number of information systems have been affected through the use of a tool designed or adapted primarily for that purpose, or else where they cause serious damage and they are committed against a critical infrastructure information"; and

"value (V) protected by privacy rights v. measures to counter offences related to terrorist activities when committed through the Internet, including social media"; and

[660] European Commission (2015), *Proposal for a Directive on combating terrorism, COM (2015) 625 final*. Here I refer to the Council Revisions of 23 February 2016.

"value (V) protected by privacy rights v. removing or blocking access to webpages publicly inciting to commit terrorist offences."

3.3.5.2 Directive 2011/36 on trafficking

Directive 2011/36 on combating trafficking in human beings[661] establishes minimum rules concerning the definition of criminal offences and sanctions in the area of trafficking in human beings and introduces common provisions to strengthen the prevention of this crime. It was adopted on the same legal bases as the Directive on the fight against child abuse (2011/92), viz. articles 82(2) and Article 83(1) TFEU. The latter openly identifies human trafficking as a serious crime of cross-border dimensions.

The Directive is silent about the use of information and communication technologies to perpetrate the crime it concerns. However, recital (15) identifies a measure to fight against such crimes. It reads: "those responsible for investigating and prosecuting such offences should also have access to the investigative tools used in organised crime or other serious crime cases. Such tools could include the interception of communications, covert surveillance including *electronic surveillance*, the monitoring of bank accounts and other financial investigations."

***

Hence, it is possible to reformulate the trade-off as:

"*value (V) protected by privacy rights v. intercepting electronic communications for the sake of investigating and prosecuting trafficking in human beings*".

3.3.6 THE NOTION OF CYBERCRIME IN UNION LAW AND RELATIONSHIP WITH CYBERCRIME CONVENTION

The brief survey of offences carried out in previous subsections leads to a number of observations.

[661] Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on Preventing and Combating Trafficking in Human Beings and Protecting its Victims, and Replacing Council Framework Decision 2002/629/JHA, OJ L 101.

The first is a reformulation of the relationship between privacy rights and security in the context of cybersecurity understood as the fight against cybercrime, which will be the basis of the analysis in chapter 4.

The second is that only Directive 2013/40 contains a *renvoi*, or connection clause[662] to the CoE Cybercrime Convention. In the words of recital 15, the Budapest Convention "is the legal framework of reference for combating cybercrime, including attacks against information systems" and hence "builds on that Convention." Not only is the Union not party to the Convention, which regulates matters of both shared competence in the AFSJ and Member States' exclusive competence, but also three Member States have not ratified it yet.[663] By contrast with other, more stringent situations of *renvoi*,[664] it may be argued that the Convention is unlikely to produce tangible legal effects within Union law, or be relied upon by the Court (see, by contrast, my reasoning as to Convention 108, chapter 7, section 1.3). Such a *renvoi* may possibly indicate instead the wish to follow CoE's initiative in the area, particularly for what concerns regulatory measures beyond the Union's competences. If the Convention were to produce effects, moreover, the Union should address its negative approach towards human rights (and the lack of rules on prevention); the only human rights clause of the Convention defers to national law as to safeguards.[665] Moreover, it is worth noting that the Council of Europe recently split the department dealing with data protection from that concerned with cybercrime.

Such a practical disconnection between the Convention and EU law could have a bearing on the meaning of 'cybercrime'. As already seen, the Convention subsumes under the term very different categories of offences, whereas in the Union instruments revised herein the term is only explicitly used with reference to offences against CIA (section 3.3.1), which is mentioned once in the main text (art. 17) and several times in the recitals.[666] In relation to Dir. 2013/40 I noted a *prima facie* connection with NIS (which I explore in greater detail in

[662] Marise Cremona, 'A Triple Braid: Interactions between International Law, EU Law and Private Law' in Marise Cremona and Hans-W Micklitz (eds), *Private Law in the External Relation of the EU* (Oxford University Press 2016).
[663] In line with recital 15, the Commission has been repeatedly encouraging Member States to ratify it.
[664] Cremona (2016), 'A Triple Braid: Interactions between International Law, EU Law and Private Law'.
[665] Drazen Dragicevic, Henrik Kaspersen and Joseph Sherwa, *Conditions and Safeguards under the Budapest Convention on Cybercrime, Discussion Paper, EU/COE Joint Project on Regional Cooperation against Cybercrime* (Council of Europe 2012). This is unfortunate in the light of article 14 of the Convention discussed in section 3.3.6, and the discussion of the rule of law in chapter 1. On the other hand, the approach whereby rights are taken into account only in relation to investigative measures overlooks the importance of prevention and may not fulfil states' obligations in relation to human rights.
[666] These are 2, 14, 15, 24, where NIS is also mentioned, recitals 25 and 26 where resilience of critical infrastructures is mentioned, and 28.

chapter four). If such a connection were to be established, then the legal meaning of cybercrime would be restricted to 'narrow' cybercrimes (section 3), thus providing strong support to my second assumption whereby narrow cybercrime is substantively different from other forms of crime in cyberspace ('broad' cybercrime, see chapter 4). This would have an immediate bearing on my research question, in the sense of restricting its scope. As a second reflection, there would be an important disconnect between law and policy documents, whereby cybercrime refers to the panoply of misdeeds in cyberspace, which could have a bearing on policy approaches.

4 CONCLUDING REMARKS

This chapter introduced the case study of cybersecurity, which presents a clear ambiguity as to the relationship between security and privacy rights, not least because of the technology involved. This makes the case interesting for the sake of studying the trade-off, the adoption of which would in any case be normatively problematic in the Union. I then surveyed the policy approach of the Union, which reflects such ambiguity, and restricted the scope of the analysis to NIS and cybercrime.

Section 3 applied what I term the methodological challenge, i.e. unpacking cybersecurity, NIS and cybercrime as they are used (or not) in several EU instruments. My primary objective was not to draw conclusions on the evolution of EU law in this area, but rather to produce as many reformulations as possible of 'security v. privacy', with a view to showing the hollowness and incoherence of the 'security' side of the trade-off equation.

The proposed reformulations of the trade-off form also the basis to reason on the role of technology (partly implicit in the reformulations, with the expression 'measures to prevent/investigate') and questions on efficiency, i.e. the other two steps of the methodological challenge which I perform in chapter 4, to which I move now.

CHAPTER 4 - CAN THERE BE RECONCILIATION BETWEEN CYBERSECURITY AND PRIVACY RIGHTS?

In chapter 3 I presented the case study of cybersecurity, I applied the normative critique to trading-off privacy rights for cybersecurity, and I performed one step of the methodological critique. In this chapter I set to ascertain whether the rights to private and family life and the protection of personal data can be reconciled with cyber-security, by answering hypothesis I (the trade-off is not an adequate explicatory tool), hypothesis II (narrow cybercrime/NIS is complementary with privacy rights), and hypothesis III (the protection of privacy rights is not at odds with broad cybercrime or investigations at large). To do so, I perform the remaining two steps of the methodological challenge. First, I ascertain whether privacy and security are the only relevant dimensions of the trade-off model, building on the 'intuition' (chapters 2 and 3) that technology is a hidden factor. Secondly, I discuss whether giving up privacy is the most efficient way to achieve security. Moreover, in this chapter I address the second assumption of the thesis, whereby on the one hand narrow and broad cybercrime differ in terms of underlying logics (with narrow cybercrime being closely related to NIS), and on the other hand, narrow and broad cybercrime face similar investigatory hurdles.

Section one tries to answer the question as to whether there can be reconciliation between security and privacy, by means of a classic legal analysis, taking as a starting point the reformulation of the trade-off developed in chapter 3. In the absence of judgments directly concerning cybercrimes, I compare the requirements enshrined in the legal instruments addressing NIS, as well as the fight against cybercrime, with the requirements contained in legislation concerning the rights to the protection of personal data and respect for private and family life. Such a comparison suggests a theoretical and legal convergence between NIS and privacy rights (hypothesis II and second assumption), but it also exposes cases of conflict between tackling cybercrime and privacy rights (hypothesis III and second assumption). Importantly, the analysis reveals that, in order to prove the 'theoretical' findings concerning hypotheses II and III, it is necessary to look into technological solutions, thus proving the inadequacy of the trade-off model (alongside other points raised in section 1).

Consequently, in section two I factor technology into the equation by examining a case study within the case study, that of deep packet inspection (hereafter DPI). The analysis of the

case study challenges the simple answers found in section one. If this does not rehabilitate the trade-off thesis, it nonetheless raises the question as to how to study the interactions between rights, security threats and measures to cope with both. This leads to discussing the role played by technology neutrality, and the fourth and last hypothesis of this thesis, which is dealt with in chapter 5.

1 THE INADEQUACY OF THE TRADE-OFF TO DESCRIBE THE RELATIONSHIP WITH PRIVACY AND CYBERSECURITY

Here I try answering the question as to whether there can be reconciliation between cybersecurity and privacy rights (hypotheses I-III) by taking as a starting point the reformulation of the trade-off relations developed in chapter 3.

In line with my second assumption (introduction, section 2), section 1.1 groups together the case of NIS with that of crimes against information systems and fraud (as explained in section 1.1.1). In the absence of EU judgments directly concerning the balance between privacy rights and cybercrimes,[667] I compare the requirements enshrined in the legal instruments addressing NIS, as well as the fight against cybercrime, with the requirements contained in legislation concerning privacy rights. The analysis of the relevant instruments unveils a convergence of protection goals that culminates in the case of data breaches and supports hypothesis II (sections 1.1.2-1.1.3.1).

Also in line with my second assumption (introduction, section 2), section 1.2 addresses the trade-off in the case of cybersecurity, when understood as the fight against cybercrimes other than those affecting information systems (hypothesis III). The requirements enshrined in the legal instruments addressing the fight against cybercrime reveal a divergence of protection goals, and the subsequent need to carry out a fundamental rights assessment (section 1.2.1). Such assessment (section 1.2.2) leads to three fundamental reflections, which enable us to dismiss the trade-off model as a theoretical instrument of limited use, because it does not

[667] One exception could be *WebMindLicenses* (discussed in section 2), but unfortunately the CJEU does not delve into the use of malware to ascertain criminal conduct, leaving it to the national judge to carry out the necessary fundamental rights analysis.

capture all potential scenarios, and misses an important part of the equation, i.e. technology, thus proving hypothesis I (section 1.3).

1.1 INFORMATION SECURITY: CONVERGENCE OF NIS WITH CIAS, AND COMPLEMENTARITY WITH PRIVACY RIGHTS

1.1.1 THE TRADE-OFF THESIS REFORMULATED: CIAS AS THE OTHER SIDE OF THE NIS COIN

In chapter 3, the methodological challenge (i.e. the reformulation of the trade-off, taking into account on the one hand the complex nature of privacy rights, and on the other the concrete challenge to security measures) led to the following results in the context of NIS:

> *"value (V) protected by privacy rights v. measures to preserve*
>
> the *availability, authenticity, integrity or confidentiality* of stored or transmitted or processed **data** or the related essential/digital services offered by, or accessible via network and information systems.
>
> the *availability, authenticity, integrity or confidentiality* of stored or transmitted or processed **data** or the related communication services offered by, or accessible via network and information systems, and the network and information systems themselves.
>
> *authenticity and integrity* of stored or transmitted or processed **data** offered by e-identification schemes and trust services, accessible via network and information systems."

As for crimes against information systems, the reformulation reads:

"value (V) protected by privacy rights v. measures to counter

access without right, to the whole or to any part of an *information system*, by infringing a security measure (Illegal access to information systems)

seriously hindering or interrupting the functioning of an *information system* by *inputting* computer **data**, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible (Illegal system interference)

the deleting, damaging, deteriorating, altering or suppressing computer **data** on an *information system*, or rendering such data inaccessible (Illegal data interference) and

the intercepting, by technical means, non-public transmissions of computer **data** to, from or within an information system, including electromagnetic emissions from an *information system* carrying such computer data (Illegal interception)."

"*value (V) protected by privacy rights v. measures to counter the* misuse of devices"

Finally, in the context of fraud, the revised trade-off reads:

"value (V) protected by privacy rights v. measures to counter

the altering, deleting or suppressing of computer **data**, in particular *identification* data, or interfering with the functioning of a computer programme or system, for the sake of procuring an unauthorised economic benefit for the person committing the offence" and

fraudulent making, receiving, obtaining, sale or transfer to another person or possession of instruments, articles, computer programmes and any other means peculiarly adapted for the commission of counterfeiting or falsifying of a payment instrument in order for it to be used fraudulently, or computer programmes the purpose of which is the commission of any of the offences described under Article 3."

The reason why I am aggregating the reformulations of the trade-off relating to NIS, attacks against information systems, and fraud, has to do with my second assumption, whereby the underlying logics of narrow cybercrime are different from 'broad' cybercrime, but are similar to NIS. Such a claim can be best understood by observing the interaction between information security canons mentioned in chapter 3 (section 1.2.2; see also chapter 5, section 3.2) and cybercrimes.

Information security canons	Loss of information security canons
Authentication: The identity claimed by users or entities can be established.	**Spoofing/identity theft**: the identity claimed by users or entities cannot be verified
Availability: Services are accessible and operational as expected;	**Interference**: the system is inaccessible or not-operational as otherwise expected
Confidentiality/secrecy: Data in transit or stored are only accessible by the intended recipient/authorized entity	**Interception**: unauthorized parties sniff data in transit/read stored data.
Control/Authorization: Only the authorized personnel can access the system/information	**Illegal access**: unauthorized parties can access the system/information
Integrity: The data transmitted or stored are unchanged and complete	**Data interference**: deleting, damaging, deteriorating, altering or suppressing data

Table 3 Information security canons and their violation

Illegal access entails a violation of authorization/control and possibly authentication; illegal system interference is the consequence of the loss of availability; illegal data interference corresponds to loss of integrity; illegal interception corresponds to loss of confidentiality. Indeed, these are typically defined as CIA crimes: crimes against confidentiality, integrity and availability of information systems. Because these crimes target the principles governing the security of information systems, they are often referred to as 'narrow', as opposed to those offences relying on computer and information systems as a means, which are referred to as 'broad' cybercrimes.[668] Likewise, (cyber)fraud entails tampering or forgery, i.e. compromising data integrity. Hence, even if fraud and forgery are typically referred to as computer-related crimes, where information systems are only a means to an end, perpetrating them requires compromising information security canons, and as a result they should be seen as a form of narrow cybercrime. In other words, NIS instruments and narrow cybercrime instruments (CIA/fraud and forgery) are intimately related. This is

[668] Henrik Kaspersen, 'Jurisdiction in the Cybercrime Convention' in Bert-Jaap Koops and Susan Brenner (eds), *Cybercrime and jurisdiction. A global survey* (TMC Asser 2006). Elaborating on such a division: Porcedda (2012), *Data Protection and the Prevention of Cybercrime: the EU as an Area of Security?* See also Gercke (2012), pp. 11-12.

confirmed by recital 2 of the Directive on attacks against information systems:[669] "Ensuring an appropriate level of protection of information systems should form part of an effective comprehensive framework of prevention measures accompanying criminal law responses to cybercrime." Such a connection is further testified by the converging definition of information systems, as I discuss in section 1.1.2 below.

To be sure, the two sets of laws differ as to the area of EU law of reference (and hence competences), and underlying logics. The first set of instruments lies on the prevent-detect-respond/analyse continuum (e.g. art. 2 (4) of ENISA Regulation[670] on objectives), laying down preventative rules for information security (which, in the economy of the internal market, internalize externalities and provide a level-playing field for actors, thus fostering fair competition). The second set of instruments criminalizes challenges to information security, and rests on the detect-investigate-prosecute continuum, thus being firmly grounded in the AFSJ (harmonization of offences and cooperation). Yet such differences do not challenge the inherent common underlying logic between narrow cybercrime and NIS. Hence, when studying their relationship with privacy rights, these instruments should be dealt with as a bundle.

1.1.2 THE LEGAL DEFINITION OF INFORMATION, AND THE LINK WITH (PERSONAL) DATA

In order to reflect on the possibility of reconciling privacy rights (as enshrined in secondary law) with cybersecurity (understood as NIS), and hence the fight against narrow cybercrime, it is first of all necessary to clarify the respective remits, beginning with the concept of information.

The possible interrelations as to 'information' are given in table 4 below. Accordingly, information can be of an indefinite nature when looked at as electromagnetic signals, which represent information's 'physical' nature and encompass all existing (e-)information. Such information can be impersonal, i.e. carrying information that does not necessarily concern an individual but rather, say, the state of a network or information collected from environmental

[669] Directive 2013/40/EU on Attacks against Information Systems.
[670] Regulation 526/2013/EU on ENISA.

sensors. Conversely, such information can be personal, i.e. concerning an individual, which represents a sub-category of all e-information.

Layers	**Information**		
Logical	Indefinite	i) Impersonal	ii) Personal
Physical	Electromagnetic emissions (signals)	Computer data (digital signals)	Personal data (digital signals)
	[Broadest category]		[Smallest category]
	Physical	Logical	
	Layer		

Table 4 Meanings of information in the field of network and information security

The secondary instruments of EU law taken into account in this study define neither information, nor signals (so much for the centrality of such concepts in the applicable law).

The notion of signals is crucial for the definition of electronic communications pursuant to art. 2 (a) of the Framework Directive:[671] networks are transmission systems and other equipment (apart from terminal equipment), which "permit the conveyance of signals by wire, radio, optical or other electromagnetic means." Even if signals are analogue at the source, circulation over electronic networks requires their transformation into digital signals.

The closest proxy to information is data, as can be evinced from the definition of information systems provided in the NIS Directive,[672] and in the Directive on attacks against information systems reported in the table below.

[671] Framework Directive (2002/21/EC).
[672] Directive 2016/1148/EU of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, OJ L 194.

NIS Directive, art. 4 (1)	Directive on attacks against info systems, art. 2 (a)
(b) Any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of **digital** data;	A device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes **computer** data, as well as **computer** data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance
OR	
(c) **Digital** data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance	

Table 5 Definition of information systems in EU law

In both instances, information systems are a device (i.e. a single computer, mobile phone, tablet, satellite, etc.) or group of interconnected or related devices that automatically process data (which can be personal). Alternatively, the information system can also coincide with the data necessary for its own functioning (which would arguably be impersonal), as per art. 4 (1) (c) of the NIS Directive and the second limb of art. 2 (a) of Dir. 2013/40 (starting with 'as well as'). Note that the broader scope of application of Dir. 2013/40 (chapter 3, sections 3.2.1 and 3.3.1) can be discounted for the sake of the argument I elaborate here.

Hence, the two instruments embody a broad definition of information, as in the table above, though they use different qualifiers of data: NIS refers to digital data (which is not defined), whereas the Directive on attacks against information systems refers to computer data. The latter are defined as "a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function" (art. 2 (b)). Digital and computer data must be understood as synonymous, in that computer data are only expressed in digital, i.e. binary, form.

The analogy between information and data can be found, or demonstrated, for other instruments. For instance, it can be argued in the case of the e-IDAS Regulation's[673] 'person

[673] Regulation 910/2014/EU on eIDAS and Trust Services.

identification data', namely "a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established" (Art. 3 (3). Here identity is information expressed in the form of data (which begs the question of the meaning of personal data *vis-à-vis* 'person identification data' in relation to natural persons).

Bearing in mind chapter 2, I believe the privacy rights' interconnection with signals, information, and data can be easily demonstrated. The link is clear in the case of the General Data Protection Regulation (hereafter GDPR).[674] Pursuant to its article 4 (1), 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. It must be recalled that personal data can express elements of private and family life. To be sure, for the purposes of this discussion, reference must be made to data processed wholly or partly by automatic means (art. 2 (a)) (the notion of personal data is further discussed in chapter 7).

The link between information and data can also be argued for communications, the confidentiality of which represents the fourth limb of article 7 of the Charter of Fundamental Rights[675] introduced in chapter 2. The definition of communications found in art. 2 (d) of the e-privacy Directive[676] reads "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service." Information should be ultimately understood as data, not least because, to be transmitted, it must ultimately be expressed in the form of digital signals, hence digital/computer data.

1.1.3 A PRELIMINARY RESPONSE TO THE RECONCILABILITY OF PRIVACY WITH CYBERSECURITY AS NIS/NARROW CYBERCRIME PREVENTION

Defining the cross-interactions between the instruments under analysis allows refining the re-formulations of the trade-off copied *supra*, section 1.1.1, which in turn is a starting point to

[674] General Data Protection Regulation (2016/679/EU).
[675] There could be a further connection between personal 'devices' and the home, which however is not of immediate relevance for the current discussion.
[676] E-Privacy Directive (2002/58/EC).

address the question as to whether it is possible to reconcile privacy rights with cybersecurity in the area of NIS/narrow cybercrime (hence hypothesis II on complementarity). Let us begin with the following re-formulations:

The (value safeguarded by the) protection of personal data v. measures to protect the *availability, authenticity, integrity or confidentiality* of stored or transmitted or processed **data** or the related essential/digital services offered by, or accessible via network and information systems; and

The (value protected by the) confidentiality of communications v. measures to counter the intercepting, by technical means, non-public transmissions of computer **data** to, from or within an information system, including electromagnetic emissions from an *information system* carrying such computer data (Illegal interception).

In the light of the explanations of the security canons (*supra*, section 1.1.1), the trade-off formulations just shown appear nonsensical: there is no *prima facie* tension between the protection of personal data with, say, the integrity of (generic) data offered by digital services. Similarly, there is no *prima facie* tension between the confidentiality of personal communications and the prevention of interception of computer data. This reading is corroborated by *Digital Rights Ireland*,[677] where the ECJ asserted that data security is the essence of article 8 of the Charter (§ 40), whereas the confidentiality of the content of communications is the essence of article 7 of the Charter (§ 39). I will discuss this further in chapters 6 and 7.

Actually, such a result is not surprising. If, following Andrade, we argue that (digital/computer) data can represent anything (chapter 3, section 1.2.2),[678] then this includes information concerning identified or identifiable individuals as well as personal communications. The sets of instruments under study are the *leges speciales* for different kinds of information: signals (Framework Directive); computer/digital data (NIS Directive, Directive on attacks against information systems and Framework Decision on Counterfeiting); personal communications (e-Privacy Directive); personal information (GDPR); e-identity and integrity of e-docs (eIDAS); payments and related authentication services (payments Directive, see *infra*). Moreover, the instruments under study are

[677] *Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*.
[678] According to Andrade (2011), 'information' not only helps make sense of complexity, but is also a foundational element of the world we live in.

predicated on the same paradigm, aim at prevention and rely on technical and organizational measures. I take each of these points in order.

All instruments, with the exception of the Framework Decision on Counterfeiting, are predicated on the same paradigm, that of risk assessment and management (chapter 3, section 1.2.3). Hence, all instruments aim at detecting risks, (i.e. vulnerabilities to threats) and avoiding them. Some examples can illustrate this more clearly. Pursuant to article 3 (d) of its Regulation, ENISA should facilitate the establishment and take-up of European and international standards for risk management and for the security of electronic products, networks and services; the related recital 33 stresses that "efficient network and information security policies should be based on well-developed risk assessment methods, both in the public and private sector…Promoting and developing best practices for risk assessment and for interoperable risk management solutions ... will increase the security level of networks and information systems" (see also recitals 19 and 24). Similarly, articles 14 and 16 of the NIS Directive lay down rules building on risk management for essential and digital services respectively. Recital 12 of the Directive on attacks against information systems sees in the "identification and reporting of threats and risks posed by cyber attacks and the related vulnerability of information systems…a pertinent element of effective prevention of, and response to, cyber attacks and to improving the security of information systems." Recital 24 stresses the importance of supplying information for the sake of performing "threat assessments and strategic analyses of cybercrime". Finally, the GDPR contains several provisions referring to risk (chapter 2, section 3.3.2, and chapter 7). References to risks are also found in article 4 on the security of processing and recital 20 (data breach) of the e-privacy Directive.

Moreover, said instruments express a logic of prevention: they aim at protecting information by means of technical and organizational measures appropriate to the seriousness of the threat and the likelihood of the risk incurred. Once more, some examples can be illustrative. One of ENISA's objectives is enhancing and strengthening capability and preparedness to prevent, detect and respond to network and information security problems and incidents (article 2 (4), art. 3 (b) and recital 23), as well as advising on using risk-prevention technologies effectively (art. 3 (d)). Similarly, the Directive on attacks against information systems aims to "facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities" (article 1); as mentioned *supra* (section 1.1.1), recital 2 stresses the complementarity between criminal and preventative

measures. Any Commission's revisions of the Directive should be based, among others, "on technological developments, for example those enabling more effective enforcement in the area of attacks against information systems or facilitating prevention or minimising the impact of such attack" (recital 25). As for the privacy rights framework, prevention is explicitly mentioned in recital 21 of the e-Privacy Directive, which reads "Measures should be taken to prevent unauthorised access to communications in order to protect the confidentiality of communications, including both the contents and any data related to such communications." Likewise, it is mentioned in recitals 39 (preventing unauthorised access to or use of personal data and the equipment used for the processing), and 83 (maintaining security and preventing infringement) of the GDPR.

Accordingly, all instruments mandate the adoption of appropriate technical and organizational measures (art. 17 Directive 95/46; art 5 and 24 GDPR; art. 4 e-Privacy Directive; arts. 14 and 16 NIS Directive; art. 19 eIDAS Regulation), or a similar locution (e.g. 'technical regulatory standards', recitals 93, 94 and 96 and art. 98 e-Payments directive), or 'technical security and data protection', art. 5 last indent of the e-Payments Directive; or measures including the protection of their information systems and associated data - recital 26 - and prevention measures, recital 2 of the Directive on attacks against info systems).

Before continuing, the position of the Framework Decision regarding counterfeiting should be clarified, as it does not contain measures aimed at preventing fraud (though prevention is mentioned in recitals 6 and 10). It can be argued that such measures are contained in the new Directive for payment services in the internal market (based on art. 114 TFEU).[679] Directive 2015/2366 does not refer to the CFD, but contains measures aimed at preventing fraud and counterfeiting. For instance, its recital 7 reads, "in recent years, the security risks relating to electronic payments have increased. This is due to the growing technical complexity of electronic payments, the continuously growing volumes of electronic payments worldwide and emerging types of payment services. Safe and secure payment services constitute a vital condition for a well- functioning payment services market. Users of payment services should therefore be adequately protected against such risks." It should therefore be regarded, in its relevant parts, as an instrument that lays down preventative measures against fraud and counterfeiting perpetrated by means of subverting information security canons, notably integrity and confidentiality. Such measures are in the form of security requirements that

[679] Directive 2015/2366/EU on Payment Services in the Internal Market.

follow a risk management/assessment approach (see article 95 and recitals 91, 92 and 96) akin to those enshrined in the instruments revised thus far.

Given the convergence of instruments, the next section focuses on identifying commonalities in organizational and technical measures and protection goals to support the preliminary response just provided. The section after identifies a clear overlap in the approach to data breaches.

1.1.3.1 Complementarity between NIS, narrow cybercrime prevention and privacy rights

Apart from provisions on security breaches, the instruments under analysis contain references to privacy rights that go beyond the mandatory recital (chapter one, section 2.3) listing the potentially affected fundamental rights.[680] I analyse three references in particular: provisions referring to respect for the applicable privacy rights-related law; rules that call for cooperation with data protection authorities; and articles spelling out the complementarity between the objective of the given instrument and privacy rights. I tackle each point in order.

First, the instruments include provisions specifying the need to respect the applicable data protection laws, which fall within a logic of reconciliation. These are art. 2 and recital 72 of the NIS Directive; recital 30 of the Directive on attacks against information systems, which mentions Article 16(1) TFEU and Article 8 of the Charter; recitals 46 and 89 of the Directive on payments and its art. 94 (2) (embodying data minimization) "payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user"; Article 67 (2) (f) of the eIDAS Regulation, which also embodies a measure of data minimization, as well as recital 11 and article 5, whose paragraph 2 actually contains a privacy rights-enhancing feature "Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited."

Secondly, several instruments contain provisions on cooperation with data protection authorities, which are a step beyond simple reconciliation. To be sure, some relate to data

[680] Examples include: recital 75 of the NIS Directive; recital 29 of Directive on attacks against information systems; and recital 90 of the Directive on payments in the internal market.

breaches or incidents that may have compromised personal data, such as art. 15 (4) and recital 63 of the NIS Directive, and 20 (2) of the eIDAS Regulation (article 17 (4)(f) and recital 31 relate instead more specifically to informing DPAs in case audits of qualified trust providers show that personal data protection rules have been breached). However, other provisions encourage wider cooperation beyond situations of emergency caused by incidents, as shown in the following examples. Article 3 (1) (d) (e) mandates ENISA to cooperate with Union agencies, including those dealing with cybercrime and the protection of privacy and personal data, with a view to addressing issues of common concern, including by: (i) exchanging know-how and best practices; and (ii) providing advice on relevant network and information security aspects in order to develop synergies. In the words of the related recital 28, "the Agency should aim to achieve synergies between the efforts of those bodies and its own efforts to promote advanced network and information security." Likewise, art. 8 (6) of the NIS Directive obliges competent authorities and a single point of contact to consult and cooperate with the relevant national law enforcement authorities and national data protection authorities. Art 8 (4) (c) of the Framework Directive recalls that supervisory bodies should contribute to ensuring a high level of protection of personal data and privacy. In a similar sense, Directive 2013/40 on attacks against information systems encourages international cooperation relating to the security of information systems, computer networks and computer data, and giving proper consideration of the security of data transfer and storage in case of international agreements involving data exchange (recital 27).

Thirdly and crucially, the instruments under analysis contain provisions that spell out the complementarity between the protection goals of privacy rights instruments and NIS/ cybercrime instruments, which I delve into in the following.

The ENISA regulation clearly links NIS with privacy rights: the Agency should contribute to both "an enhanced level of security of electronic communications as well as of privacy and personal data protection" (recital13) and "a high level of network and information security, to better protection of privacy and personal data, and to the development and promotion of a culture of network and information security." Recital 15 spells out that instruments disciplining privacy rights contain measures complementary to NIS. As for the e-privacy Directive, the Regulation refers to article 4, which "requires a provider of a publicly available electronic communications service to take appropriate technical and organisational measures to safeguard the security of its services" and to article 5 (3) which "requires that the confidentiality of the communications and related traffic data be maintained." The ENISA

Regulation also refers to provisions on personal data breaches and notification that I discuss in the next section. Recital 15 also refers to the technical and organisational measures enshrined in article 17 of Directive 95/46/EC "to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network and against all other unlawful forms of processing." Such measures have been retained and extended in chapter 4 of the GDPR, which now contains an obligation to adopt personal data protection measures by default and design (art. 25) and to actively pursue anonymization.

Recital 26 of the Directive on attacks against information systems encourages Member States to take the

> *"necessary measures to protect their critical infrastructure from cyber attacks, as part of which they should consider the protection of their information systems and associated data. Ensuring an adequate level of protection and security of information systems by legal persons, for example in connection with the provision of publicly available electronic communications services in accordance with existing Union legislation on privacy and electronic communication and data protection, forms an essential part of a comprehensive approach to effectively counteracting cybercrime. Appropriate levels of protection should be provided against reasonably identifiable threats and vulnerabilities in accordance with the state of the art for specific sectors and the specific data processing situations."*

Recital 6 acknowledges the link between large-scale cyber attacks and "the loss or alteration of commercially important confidential information or other data". Moreover, the Directive opens up the possibility of using the loss of compromising of personal data as an aggravating factor to cybercrimes. For instance, it could qualify damage caused by botnets as serious crime (recital 5). Pursuant to article Art. 9 (5), committing illegal system or data interference "by misusing the personal data of another person, with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner" could be regarded as aggravating circumstances.

The eIDAS Regulation contains a number of provisions suggesting complementary between security and privacy rights. Recital 4 spells out that "authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online. Furthermore, requirements under Directive 95/46/EC concerning confidentiality and security of processing should be respected by trust service providers and supervisory bodies." Article 12 (3) (c) refers to the

implementation of the principle of privacy by design. Trust service providers should, pursuant to art. 24 (2) (b), employ staff who have received appropriate training regarding security and personal data protection rules.

Furthermore, the Directive on payments also lists a number of requirements suggesting complementarity between security and privacy. According to recital 89, all data processing systems developed and used should embed data protection by design and data protection by default. The payment initiation service providers and the account information service providers, as well as the account servicing payment service provider, should observe the necessary data protection *and* security requirements (recital 93). The European Banking Authority should "systematically assess and take into account the privacy dimension, in order to identify the risks associated with each of the technical options available and the remedies that could be put in place to minimise threats to data protection" when "developing regulatory technical standards on authentication and communication" (recital 94). Article 5 expresses rules on the security policy document, which should include "a description of security control and mitigation measures taken to adequately protect payment service users against the risks identified, including fraud and illegal use of sensitive and personal data". Art. 5 (1) (j) a) indicate "how they ensure a high level of technical security and data protection, including for the software and IT systems used by the applicant or the undertakings to which it outsources the whole or part of its operations" (art. 5 last indent). Art. 97 (3) on authentication obliges Member States to ensure that payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials. Finally, art. 98 (2) on technical standards on authentication and communication must, among others (b) ensure the safety of payment service users' funds and personal data.

1.1.3.2 The obvious overlap: data breaches

Provisions concerning NIS, the fight against narrow cybercrimes and both sets of privacy rights manifestly overlap in the case of 'data breaches'. Data breaches feature almost daily in newspapers, and range from the violation of security of email providers, to cloud repositories, etc.

The notion of data breaches acquired legal significance with the amendment of the e-privacy Directive in 2009,[681] when art. 2 (i) was introduced. Accordingly, data breaches are "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community." Art. 4 (12) of the GDPR broadens the scope of personal data breaches beyond publicly available electronic communications services.

A security breach is a specific form of incident, i.e. 'any event having an actual adverse effect on the security of network and information systems' (NIS Directive art. 4 (7)), including personal data as acknowledged by recital 63 ("personal data are in many cases compromised as a result of incidents"). In this respect, the breach is system-specific; for instance, in the context of electronic identification services, it consists in the breach or partial violation of the electronic identification scheme or authentication so as to affect the reliability of the cross-border authentication of that scheme (art. 10 eIDAS Regulation).

A security breach corresponds to data interference (destruction, loss or alteration of data) and illegal access (unauthorized access) in the sense of the Directive on attacks against information systems. Recital 85 of the GDPR lists the offences that could ensue were a personal data breach not to be addressed in an appropriate and timely manner, including "physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

Due to the potential leakage of personal and impersonal information, the risk of security breaches is treated with the utmost severity. The different instruments follow the same blueprint, composed of the following three steps.

The first is prevention: the adoption of appropriate technical and organizational measures proportionate to risks to prevent and minimize the impact of incidents. This includes, for

[681] 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.

instance in the sector of payment services,[682] 'strong customer authentication' as a measure to prevent fraud, i.e. an authentication based on the use of two or more elements[683] that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data (art. 4 (30)). Recital 96 clarifies that such measures typically include encryption. According to art. 4 of the Commission Regulation on data breaches,[684] data controllers do not have to notify a data breach if it has taken measures that render the data unintelligible to unauthorised parties. Such measures, which are not to be considered *per se* exhaustive of the security obligations of data controllers, are laid down in the second paragraph: encryption with standardized key (letter a), or replacement of data by its hashed value calculated with a standardised cryptographic keyed hash function (letter b).

The second step is minimization: in case of breaches, the affected party must inform the responsible bodies so as to agree on measures to contain further damage. Obligations may vary in respect of the importance of the service, and the expected degree of control Member States have on service providers. The eIDAS Regulation openly states "Notification of security breaches and security risk assessments is essential with a view to providing adequate information to concerned parties in the event of a breach of security or loss of integrity" (Recital 38). In the context of electronic identification, article 10 (1) prescribes that "Where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission." The same applies to trust services. Pursuant to article 19 (1), first indent, "Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein."

[682] Directive 2015/2366/EU on Payment Services in the Internal Market.
[683] Categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is).
[684] Commission Regulation 611/2013/EU of 24 June 2013 on the Measures Applicable to the Notification of Personal Data Breaches under Directive 2002/58/EC of the European Parliament and of the Council on Privacy and Electronic Communications (Commission Regulation on Data Breaches). The Regulation is supposed to be revised in 2016 and is likely to be overhauled with the revision of the e-privacy Directive.

Operators of essential services have to swiftly notify the competent authority or the CSIRT (hereafter Computer Security Incident Response Team) of incidents having a "significant impact on the continuity of the essential services they provide" (article 14 (3) NIS Directive). Operators of digital services must swiftly notify the competent authority or the CSIRT of incidents when they offer their services to essential service operators (art. 16(5) NIS Directive). As for other incidents, the obligation to notify must fulfil two cumulative requirements: the incident must have a "substantial impact on the provision of a service" (art. 16 (3) NIS Directive), and the provider has "access to the information needed to assess the impact of an incident against the parameters" established by the Directive (art. 16 (4) of the NIS Directive); this may reflect the reality of a market composed of mostly non-EU service providers.

The third step is that of informing the public. For instance, Article 19 (6) of the NIS Directive lays down that, "after consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an on-going incident." Depending on the gravity of the breach, and the liability of the breached party, this could be akin to 'naming and shaming', in that the breached party may have to notify the breach to affected individuals/entities. In the context of trust services, the second indent of article 19 (2) of the eIDAS Regulations lays down that, "where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay."

An additional step, which however is more pronounced in the case of personal data breaches, consists of liability and sanctions: the breached party is exposed to sanctions depending on the degree of responsibility (i.e. not having taken the necessary measures) or the importance of the service offered. For instance, art. 83 (2) (d) of the GDPR ties administrative fines to "the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32", namely the rules on data protection by default and by design, and on the security of the processing. If, pursuant to art. 83 (4) (a), the data controller or processor has infringed these provisions, but also those of notification of data breaches, and cannot prove "that it is not in any way responsible for the event giving rise to the damage" (art. 82), it is liable to paying the highest administrative fines (up to 10 000 000 EUR, or in the case of an undertaking, up to 2

% of the total worldwide annual turnover of the preceding financial year, whichever is higher).

1.1.3.3 A preliminary response to hypothesis II

The analysis carried out in the previous paragraphs seems to confirm that privacy rights and cybersecurity (understood as NIS) and the fight against narrow cybercrime are easily reconciled. In the introduction to this thesis I proposed three different understanding of reconciliation: convergence, overlap and causation.

The provisions revised in section 1.1.3.1 are a strong indication that there can be, at a minimum, convergence between narrow cybercrime/NIS and privacy rights. The analysis conducted in section 1.1.3.2, moreover, indicates that there is an area of complete overlap, that of data/security breaches. It is not possible to find a conclusion on causation, i.e. that the obligations stemming from privacy rights-related instruments, and particularly the technical and organizational measures, are a proxy in ensuring cybersecurity, or vice versa. It would be necessary to analyse the specific measures, particularly the technical ones, which do not fit in a generic trade-off discussion. The analysis of specific measures would moreover reinforce the findings concerning the other two types of complementarity.

My second assumption, however, mentions the fact that, when it comes to the investigation of cybercrimes, broad and narrow cybercrimes tend to converge; the peculiarity of data as evidence is reflected in the instruments harbouring reconciliation between privacy and security.

Recital 23 of the Directive on attacks against information systems points to the need to cooperate with service providers to preserve potential evidence, provide elements helping to identify offenders and eventually shut down, completely or partially, information systems or functions that have been compromised or used for illegal purposes. Art. 94 (1) of the Directive on payment services lays down that “Member States shall permit processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation and detection of payment fraud”, obviously in accordance with applicable law. The same GDPR contains a clause, recital 49, whereby “the processing of personal data to the extent strictly necessary and proportionate for the purposes

of ensuring network and information security…and the security of the related services offered by, or accessible via, those networks and systems" constitutes a legitimate interest of the data controller, without any references to the ensuing personal data protection benefits. Finally, article 1 (3) second indent of the Framework Directive recalls that measures regarding end-users' "access to, or use of, services and applications through electronic communications networks are liable to restrict fundamental rights or freedoms, and may only be imposed … with due respect for the principle of the presumption of innocence and the right to privacy."

It seems more appropriate, however, to discuss these issues in the context of the next section, which concerns cybercrimes where 'cyberspace' matters only as the crime scene providing evidence (and the related hypothesis III).

1.2 (CYBERSECURITY AS) THE FIGHT AGAINST BROAD CYBERCRIME

1.2.1 THE TRADE-OFF BETWEEN PRIVACY RIGHTS AND CYBERSECURITY AS THE FIGHT AGAINST CYBERCRIMES

The methodological challenge (i.e. the reformulation of the trade-off taking into account on the one hand the complex nature of privacy rights, and on the other the concrete challenge to security), applied in chapter three to 'broad' cybercrimes, led to the following results.

In the context of abuse against children:

"value (V) protected by privacy rights v. measures to

remove web pages containing or disseminating child pornography hosted in their territory and to endeavour to obtain the removal of such pages hosted outside of their territory; and

block access to web pages containing or disseminating child pornography towards the Internet users within their territory."

In the context of terrorism:

> "*value (V) protected by privacy rights v. measures to*
>
> counter illegal system interference or illegal data interference where a significant number of information systems have been affected through the use of a tool designed or adapted primarily for that purpose, or else where they cause serious damage and they are committed against a critical infrastructure information (large-scale cyber attacks); and
>
> counter offences related to terrorist activities when committed through the Internet, including social media; and
>
> removing or blocking access to webpages publicly inciting to commit terrorist offences."

In the context of human trafficking:

> "value (V) protected by privacy rights v. intercepting electronic communications for the sake of investigating and prosecuting trafficking in human beings."

Apart from large-scale cyber attacks, which belong more naturally in the narrow cybercrime category as they concern threats to information systems, all other reformulations of the trade-off embody threats which pertain not to information, but rather to human conduct (child abuse or pornography, human trafficking, recruitment of terrorists), where network and information systems may act as an amplifier or conduit, but that does not require subverting information security canons (or else the physical infrastructure of the network). Hence, as anticipated *supra* (section 1.1.1), offences where the use of network and information systems are an incidental element, or a dumb means, are typically referred to as broad cybercrimes (which I assume to be different from narrow cybercrimes).

In this respect, the question as to whether there can be convergence between privacy rights and cyber-security (when understood as the fight against broad cybercrimes) cannot be resolved by highlighting common protection goals. The only exception may be found in the case of audio-visual material portraying child pornography (because images are personal data, as discussed in chapter 7). The prevention of broad cybercrimes does not rest primarily on technical measures, but rather on societal action, which could make use of network and information technologies as a medium. By means of an example, article 23 of the anti-child

abuse Directive[685] mandates Member States to take actions such as education and training to discourage any form of abuse against children (§ 1), or else to provide information and organize awareness-raising campaigns, including through the Internet, and foster research and education programmes aimed at reducing the risk of children becoming victims of sexual abuse or exploitation (§2). Along similar lines, awareness that radicalisation of terrorists takes place in prisons[686] demands preventative measures aimed at penal institutions, though the proposed Directive on counter-terrorism[687] does not contain provisions in this sense.

Unlike the discussion on NIS/narrow cybercrimes, no simple answers can be derived from the recitals/text of the instruments either, which do not include special mentions of the rights to respect for private and family life, and protection of personal data, apart from the clause, mandatory for Union law, ensuring the respect for fundamental rights and observance of the principles recognised in particular by the Charter (see chapter 1, section 2.3). Such clauses are found in recital 50 of the anti-child abuse Directive, recital 19 of the proposed Directive on counter-terrorism, recital 33 of the Directive against human trafficking (but which surprisingly does not refer to respect for private life), and recitals 12 and 18 of the latest amendment to the copyright Directive.[688]

Returning to the issue of prevention, the absence of provisions of that kind is not surprising, given that all instruments find their legal basis in the AFSJ, typically articles 82 and 83 on judicial and police cooperation in criminal matters. Hence preventative measures are not the focus of such instruments, and if they feature in them, it is usually in a minor role. In line with EU competences, which cannot encroach upon Member States' prerogative of providing law and order (chapter 1, section 2.4), these instruments harmonize minimum definitions of offences and provide for mechanisms of cross-border cooperation.

---

[685] Directive on Combating Child Sexual abuse, Exploitation and Pornography (2011/92/EU).

[686] Rachida Dati, (Rapporteur), *Draft Report on prevention of radicalisation and recruitment of European citizens by terrorist organisations (2015/2063(INI))* (European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 2015).

[687] European Commission (2015), *Proposal for a Directive on combating terrorism, COM (2015) 625 final*.

[688] European Commission, *Proposal for a Directive of the European Parliament and of Council on Certain Permitted Uses of Works and Other Subject-matter Protected by Copyright and Related Rights for the Benefit of Persons who are Blind, Visually Impaired or Otherwise Print Disabled and Amending Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society* ((Communication) COM/2016/0596 final, 2016). Updates can be retrieved at the following permalink: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0596.

One common measure of cooperation is exchange of information,[689] typically through Europol.[690] Such information can be both impersonal and personal, and can concern private life. This is where measures of cross-border cooperation are likely to interfere with privacy rights; the matter is relevant, however, for any type of cross-border cooperation for judicial and criminal matters, including the case of NIS/crimes against CIAs.

In other cases, the instruments are vague as to the tools that can be made use of, e.g. art. 15 (3) of the anti-child abuse Directive: "Member States shall take the necessary measures to ensure that effective investigative tools, such as those which are used in organised crime or other serious crime cases are available to persons, units or services responsible for investigating or prosecuting offences referred to in Articles 3 to 7", which is replicated, *mutatis mutandis*, in art. 21 of the proposed Directive on counter-terrorism. As discussed throughout chapter one, measures of investigation and enforcement at large are by definition likely to interfere with privacy rights, at least of the suspect(s), and call for balancing in the light of the RoL.

Some laws provide for more specific counter-measures (in a cross-border fashion, or for private actors) relating to cyberspace, as exemplified in the reformulation of a number of the trade-off relationships above. Hence, for the purposes of the current analysis, I will limit myself to the counter-measures of the type explicitly mentioned by the instruments under analysis (interception, blocking or removing web pages, and intervention on social media) to assess the reconcilability of privacy rights with cyber-security, when understood as the fight against broad cybercrime.

1.2.2 Reconciling the fight against broad cybercrimes with privacy rights

The easiest measure to appraise is that contained in the recital of the Directive against human trafficking, namely intercepting electronic communications for the sake of

[689] E.g. pursuant to Council Framework Decision 2006/960/JHA of 18 December 2006 on Simplifying the Exchange of Information and Intelligence between Law Enforcement Authorities of the Member States of the European Union, OJ L 386; Peers (2011), pp. 914-915.
[690] Regulation 2016/794/EU of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135.

investigating and prosecuting trafficking in human beings (whose validity as a legal basis I address in section 2.4.3). Interception consists in an interference with the confidentiality of communications enshrined in article 7 of the Charter, and article 5 (1) of the e-privacy Directive, which mandates Member States to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned. The scope of this right can be restricted in the cases listed in Article 15(1) to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. Three reflections ensue.

The first is that such occurrences could engender a situation of pure trade-off if pursued in contempt of the principles of necessity, appropriateness and proportionality within a democratic society, and the general principles enshrined in article 2 TEU. Directive 2016/680[691] remedies this situation by providing a framework for the processing of personal data in the field of law enforcement mandating minimum safeguards. In this respect, a pure trade-off is avoided in favour of a form of balancing capable of protecting the essence of privacy rights (thus reinforcing hypothesis III, in the form of permissibility).

The second and third reflections are interrelated. On the one hand, and second, intercepting data subverts, first of all, the information security canon of confidentiality/secrecy. There are different ways of achieving surveillance, e.g. tapping the network, which subverts the information security canon of authorization/control and potentially authentication, and the use of honeypots.[692] A different way consists in placing malware, e.g. a Trojan horse, in a suspect's device (terminal or network equipment), which affects the information security canons of authentication and integrity. Hence this situation creates an emergent clash (trade-off?) between two security requirements, which Landau aptly defined as surveillance v. security[693] and which, following the Venice Commission,[694] could be termed 'cybersecurity v.

[691] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data, and Repealing Council Framework Decision 2008/977/JHA, OJ L 119/89.
[692] Flanagan and Walden (2003).
[693] Landau (2010), *Surveillance or Security?* Here I follow the definition of surveillance proposed within the SURVEILLE FP7 project, namely "the targeted or systematic monitoring of persons, places, items, means of transport or flows of information, in order to detect specific, usually criminal, forms of conduct, or other hazards, and enable, typically, a preventive, protective or reactive response, or the collection of data for preparing such a response in the future." SURVEILLE Project Consortium (2011), p. 5.

SIGINT". As envisioned by the Parliament in its Resolution on mass surveillance,[695] the attempt to fight crime can endanger CII.

On the other hand, and third, this depends especially on the technological solution chosen. Placing a Trojan horse in someone's device endangers the information security of their system, which can be justified by the opposing imperative of fighting serious crime, provided it is done proportionately. Proportionality implies that the Trojan, or other malware, is somehow de-installed or de-activated once it is of no more use. Failure to do so would mean exposing the device to other attacks, e.g. becoming a zombie part of a botnet (in itself a cybercrime) that commits other cybercrimes, or exposing other users if the machine is a server. Tapping the network requires the use of specific hardware or the cooperation of telecommunications companies. This solution is labour-intensive and time-consuming, hence expensive. Indeed, temptation leads to a resort to catchall solutions like the NSA/GCHQ programmes, or permanent capabilities like requesting exceptional access. The risks to information security of exceptional access and the NSA/GCHQ programmes are serious for network and information security as CII.

Let us now look into the other actions: removing web pages containing or disseminating child pornography/terrorist material, blocking access to web pages containing or disseminating child pornography/terrorist material, and countering offences related to terrorism on social media.

Removing or blocking web pages do not seem, *prima facie*, privacy rights-endangering activities. The same could be said of activities of intelligence agencies on social media, which can be performed through open source intelligence and social engineering (e.g. infiltrating a group), or social network analysis (e.g. one's network of acquaintances).[696] Yet, the second set of reflections concerning interception is valid here, too. Removing or blocking web pages can also be achieved (and countered) through different technological avenues, e.g. TCP/IP header filtering, TCP/IP content filtering, HTTP proxy filtering, DNS tampering and keyword searching, as well as hybrid techniques that combine elements of each.[697]

---

[694] Council of Europe (2015).
[695] European Parliament (2014), *Resolution on the US NSA Surveillance Programme*.
[696] See Porcedda in Martin Scheinin and others, *Annex 3 to SURVEILLE Project Deliverable D 2.6 (matrix of surveillance technologies): fundamental rights technology assessment sheets (EUI)* (2013).
[697] See, among others, Christopher Marsden, 'Internet Service Providers. Content, control and neutrality (chapter 15)' in Ian Walden (ed), *Telecommunications law and regulation (4th edition)* (Oxford University Press 2012); Ross Anderson and Steven J. Murdoch, 'Tools and Technology of Internet Filtering' in John Palfrey Ron

As a result, hypothesis III, i.e. the question as to whether privacy rights can be reconciled with cybersecurity, when understood as the fight against broad cybercrimes (and the collection of e-evidence at large) cannot be answered without looking into technology. This finding is sufficient to reach some preliminary conclusions about the trade-off.

1.3 INTERIM CONCLUSIONS: THE TRADE-OFF DOES NOT CAPTURE THE RELATIONSHIP BETWEEN CYBERSECURITY AND PRIVACY RIGHTS

The analysis conducted thus far leads to the conclusion that the trade-off model is not an adequate intellectual device to capture the relations between privacy rights and (cyber)security, because it fails to factor in technology and its implications. Hypothesis I is thus confirmed without the need to look into the efficiency of 'security v. privacy'.

The temptation to downgrade the importance of technology as an element specific to cybersecurity is easily dispelled, by noting that the collection of evidence necessary to fight crimes of all forms increasingly relies on ICTs, as testified by the defunct Data Retention Directive and requests for exceptional access. Even when network and information systems are not relied upon, technology is heavily used in policing.[698] Moreover, technology is part of those 'technical measures' necessary to enhance NIS and privacy rights. As a result, the trade-off does not capture situations in which there is complementarity (convergence/overlap) between the two objectives as expressed in specific legal instruments, in this case those concerning NIS and narrow cybercrime.

The case of broad cybercrimes may fall within the trade-off model, but the availability of instruments pursuing proportionality enables avoiding a dichotomous approach. In its coarseness, the trade-off overlooks the fact that trading-off privacy rights for the sake of fighting broad cybercrimes may actually backfire, in that it could endanger the security of network and information systems on which so much critical infrastructure rests. This suggests

---

Deibert, Rafal Rohozinski, and Jonathan Zittrain (ed), *Access Denied: The Practice and Policy of Global Internet Filtering* (The MIT Press 2008); Ian Brown, 'Internet censorship: be careful what you ask for' (2008) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1026597>.

[698] See the wide array of technologies available to law enforcement authorities to fight petty or serious crime, and terrorism, analysed by the SURVEILLE project.

that 'security v. privacy' may be highly inefficient, thus adding to the findings that the trade-off is an inadequate intellectual device (hypothesis I).

In order to prove hypothesis III, as well as causation in the case of hypothesis II, it is necessary to factor in the technology involved. Moreover, an analysis of technology could validate the findings on complementarity in the sense of a convergence/overlap, making such findings bulletproof. Factoring in the analysis of technology is not only necessary to defy the trade-off model, but it is also needed to understand the issues at stake in the relationship between privacy rights and cybersecurity. The next section hence intends to remedy such an absence by looking into a case study within the case study: deep packet inspection. In doing so, I also advance a critique of classic legal analysis, leading to hypothesis IV.

2 THE NEED TO FACTOR IN TECHNOLOGY: THE CASE OF DEEP PACKET INSPECTION[699]

In this section I appraise the case of deep-packet inspection (DPI), a technology that seems to the point because it can be used both for narrow cybercrime/NIS and broad cybercrime. DPI has recently attracted the attention of regulatory bodies,[700] as well as the global media because of its use in the NSA-related surveillance scandals.[701] After describing DPI (section 2.1) and its relation with privacy rights (section 2.2) I revise its use in relation to cybercrime (section 2.3). The analysis of the legal permissibility of DPI based on applicable law and existing judgments leads to a paradox, whereby DPI appears to be, in principle, both permissible and impermissible (section 2.4). This introduces hypothesis IV, namely that the appraisal of the impact of technologies into fundamental rights cannot be *solely* based on parameters deriving from applicable law and specific judgments.

[699] An earlier and substantially different version of this section appeared within Porcedda (2013), 'Lessons from PRISM and Tempora'.
[700] International Telecommunication Union (ITU-T), *Requirements for deep packet inspection in next generation networks, Recommendation ITU-T Y.2770* (2012).
[701] For a description of the use of DPI in the NSA scandals, see Cayford (2014).

2.1 DPI: NATURE AND USAGE

According to Clarke,[702] 'well behaved' intermediary nodes in the core of the internet use their router software solely to look into the IP header of the packet (i.e. the outer envelope which contains the addressing information of the message to be sent) and either deliver the message or pass it to another node that can deliver it. DPI is a technique placed in network internal nodes[703] empowering Internet Service Providers (hereafter ISPs) to actively perform additional functions, by screening the application layer of packets, and even its payload, viz. content (hence the term 'deep'), sent over the networks. The ITU-T, which adopted requirements specifying 'technical characteristics' for DPI (in NGNs), defines it as "analysis, according to the layered protocol architecture OSI, of payload and/or packet properties deeper than transport layer header information, and other packet properties in order to identify the application unambiguously". [704] This challenges the broad version of the end-to-end argument or 'net neutrality', i.e. the idea that the lower layers involved in the core function of the internet should be unaware of the data they carry and unable to control them.[705]

Clarke notes there could be good reasons to use DPI, e.g. enhancing the Internet infrastructure: DPI (scanning the application header/payload) enables an ISP to act as a proxy-server at the request of the end-user to filter spam or webpages, provide firewalls or anonymous remailers or else reverse-proxy.[706] Indeed, DPI evolved from shallow and meso-packet inspection tools (looking solely into IP, for the destination address, and TCP, e.g. for port numbers suggesting the application used), and started being distributed a decade ago to detect and prevent malware.[707] Another positive use of DPI, albeit where users' consent needs to be addressed, is that of ISPs acting as a gateway between the Internet and other networks or for caching popular web pages. Yet, Clarke[708] notes there are also circumstances in which DPI is performed without the end users' knowledge and at their detriment. The application header and payload can be screened for: email addresses to build mailing lists of spam, or to

[702] Roger Clarke, *Deep Packet Inspection: its nature and implications* (www.rogerclarke.com 2009).
[703] Body of European Regulators for Electronic Communications (BEREC), *A Framework for Quality of Service in the scope of Net Neutrality* (BoR (11) 53, 2011), pp. 18-20.
[704] International Telecommunication Union (ITU-T) (2012), p. 5.
[705] Van Schewick (2010).
[706] Clarke (2009), *Deep Packet Inspection: its nature and implications*.
[707] Ralf Bendrath, 'Global Technology Trends and National Regulation: Explaining Variation in the Governance of Deep Packet Inspection' (International Studies Annual Convention, New York City, 15-18 February 2009). Body of European Regulators for Electronic Communications (BEREC) (2011).
[708] Clarke (2009), *Deep Packet Inspection: its nature and implications*.

sniff credit card details; changing the content of the message and sending it forward;[709] or else pretending to be the recipient of the message and forging a response; or for surveillance.

Actually, it is the surveillance capabilities that may have made DPI so attractive to private actors and law enforcement. For instance, DPI seemed suitable to fulfil the legal requirements of the United States Communications Assistance for Law Enforcement Act (CALEA), whereby all ISPs must install any available technologies enabling lawful wiretapping.[710] Either with a view to recover the investment,[711] or pushed by 'Google envy',[712] companies began using DPI for lucrative services. Examples include ad-injection (the evolution of behavioural advertising[713]) and traffic prioritization in the guise of 'network management'.[714] In turn, organizations interested in the protection of digital property rights lobbied for its use, and it was soon apparent that DPI could be used for policing the networks from all sorts of content deemed unlawful: material offending the (culture-sensitive) definition of morals,[715] such as pornography; the expression of hatred; child pornography; or material consisting in (regime-sensitive) subversive speech. In other words, DPI represented a new and powerful means for old ends.[716]

All such options are possible because, in the words of Mueller, DPI is an "enabling technology",[717] in that its function depends on the applications or modules installed in the DPI engine (its central part): recognition, notification and manipulation.

---

[709] This is what Comcast did in 2007 to block peer-to-peer networks: it "sent 'reset' TCP packets in the place of end users". Body of European Regulators for Electronic Communications (BEREC) (2011), p. 29.
[710] Ibid, p. 28.
[711] Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance, Working Paper n. 8-22* (University of Colorado Law School 2008) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1261344>; Landau (2010), *Surveillance or Security?*
[712] Landau (2010), *Surveillance or Security?* However, Google's ad injection does not come easy: Joe Mullin, 'Privacy Lawsuit over Gmail Will Move Forward' (16 August 2016).
[713] Ohm (2008).
[714] Traffic prioritization is part of network management, i.e. all actions (and tools) to administrate, operate and maintain networked systems. Bendrath (2011). Traffic management can have legitimate objectives, i.e. avoiding congestion, but it can be performed according to less intrusive means than DPI, such as application-agnostic measures. Ohm (2008), 51.
[715] Body of European Regulators for Electronic Communications (BEREC) (2011).
[716] Yaman Akdeniz, *Report. Freedom of Expression on the Internet. A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States* (2011).
[717] Milton Mueller, *DPI technology from the Standpoint of Internet Governance Studies: an Introduction (v1.1). The Network is Aware* (Syracuse University School of Information Studies, 2011), 2; Ralf Bendrath and Milton Mueller, 'The End of the Net as We Know it? Deep Packet Inspection and Internet Governance' (2010) 13 New Media and Society 1142; Ronald W. Del Sesto, Jr., and Jon Frankel, 'How Deep Packet Inspection Changed the Privacy Debate' Office of the Information & Privacy Commissioner of Ontario, Canada, 2008 previously at: <http://dpi.priv.gc.ca/>); Tim Berners-Lee, 'No Snooping' (<http://www.w3.org/DesignIssues/NoSnooping.html>, 2009); Bendrath (2011); Angela Daly, 'The Legality of

Recognition uses data mining algorithms to analyse, on- and offline, any parts of the packets, at any layer of the Internet architecture, against specific patterns or features (keywords or 'signatures' contained in a predefined library), and compares the obtained data on the basis of such patterns and keywords. According to the ITU-T requirements, the signature can be used for approximate identification, such as behavioural elements or heuristics, and exact matching.[718]

Notification consists in sending alerts in relation to the patterns and keywords identified, and is usually conducted offline. DPI engines combining recognition and notification are called 'passive'.

Manipulation, or 'active' DPI, affects the destination of the packets and can be performed both on- and offline. DPI engines can also be looked at from the angle of the hierarchical level at which they apply and whether they are used *in situ* or remotely. Packet path level actions include: accepting the packet and forwarding it to the packet forwarding function, discarding the packet (silently or otherwise); redirecting the packet to other output interfaces; replicating/mirroring the packet to other output interfaces; classifying traffic, local measurements, and reporting of measurement data; and prioritization, blocking, shaping and scheduling methods of individual packets. Node level actions include: dynamic building of new DPI policy rules and/or modification of existing rules; generating of logging/tracing data and reporting to policy management; detecting and reporting of unidentifiable applications; notifying intrusion detection systems (e.g., by reporting traffic samples, suspicious packets). Network level actions include: resource management, admission control and high-level filtering (at the level of network subsystems) and content charging based on subscribers' application types.[719] The latest evolution of DPI, which is deep content inspection, performs its analysis on the reconstructed packet.

Deep Packet Inspection' (First Interdisciplinary Workshop on Communications Policy and Regulation 'Communications and Competition Law and Policy – Challenges of the New Decade', University of Glasgow, 17 June 2010); Ohm (2008).

[718] International Telecommunication Union (ITU-T) (2012), p. 10.

[719] Ibid, p. 12.

2.2 THE RELATION BETWEEN DPI AND PRIVACY RIGHTS

The packets screened by DPI carry data produced in the course of "personal Internet usage"[720] and communications (e.g. e-mails or Voice over Internet Protocol, VOIP), which contain information susceptible to identifying an individual, such as the IP address.[721] Hence, their collection represents an interference with the right to the protection of personal data (art. 8 of the Charter).[722] Moreover, "personal Internet usage" and communications fall within the broad definition of "communication" ("correspondence"[723] in the language of the ECHR[724]), an attribute (see chapter 6) of the right to respect for private and family life (to be interpreted in line with the case law relating to article 8 ECHR). The monitoring of information produced in the course of communications, including traffic and location data,[725] constitutes an interference with the right to private life irrespective of whether the correspondence is private.[726] In *Digital Rights Ireland* (§ 39), the ECJ said the content of a communication represents the essence of art. 7 of the Charter. Furthermore, individuals have a reasonable expectation of privacy if there is no warning about the monitoring of 'correspondence'.[727] What is more, the ITU-T warns that "The mechanism described in this Recommendation may not be applicable to the international correspondence in order to ensure the secrecy and sovereign national legal requirements placed upon telecommunications, and ITU Constitution and Convention."[728]

[720] Copland v. the United Kingdom, n. 62617/00, CE:ECHR:2007:0403JUD006261700, para 41.
[721] Judgment of 24 November 2011 in Scarlet Extended, C-70/10, EU:C:2011:771, para 51.
[722] Judgment of 16 February 201 in Sabam, C-360/10, EU:C:2012:85, para 45.
[723] *Copland v. the United Kingdom, n. 62617/00*, para 41.
[724] Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocols No 11 and 14), Council of Europe, ETS n° 005, 4 November 1950.
[725] "…the use of information relating to the date and length of telephone conversations and in particular the numbers dialled can give rise to an issue under Article 8 as such information constitutes an "integral element of the communications made by telephone". The mere fact that these data may have been … in the form of telephone bills, is no bar to finding an interference with rights guaranteed under Article 8 (ibid)." *Copland v. the United Kingdom, n. 62617/00*, para 43.
[726] Niemietz v. Germany, n. 13710/88, CE:ECHR:1992:1216JUD001371088, para 32.
[727] See, for instance, *Copland v. the United Kingdom, n. 62617/00*, para 42.
[728] International Telecommunication Union (ITU-T) (2012), p. 1.

2.3 THE EXISTENCE OF A LAW PROVIDING FOR THE INTRUSION FOR THE SAKE OF CYBERCRIME

Since DPI is susceptible of interfering with privacy rights, it should only be allowed if it fully complies with a test for permissible limitations (chapter 1, section 2.3, and chapter 5, section 3.4).[729] Accordingly, the first requirement pursuant to art. 52 (1) of the Charter, is that the intrusion must be provided for by the law (or in accordance with the law, art. 8 (2) ECHR).[730] Is there a law providing for such intrusion in the European Union for the sake of cybercrime?

As seen in chapter 3 (section 3), the Union is not a party to the Budapest Convention (hereafter the Convention), however it regards it as the "international standard for cooperation and a model for national and EU legislation",[731] arguably not only on substantive but also on procedural matters. Article 21 of the Convention, once transposed into national law, could act as a legal basis allowing for use of DPI: states can enable 'service providers', in the case of serious offences, to conduct real-time (confidential) interception ('collection or recording') of content data, relating to specified communications transmitted by means of a computer system. The expression 'in the case of serious offences' could be interpreted in a restrictive manner and relate solely to the investigation of serious offences, or in a broader sense to include preventative actions (though the Convention does not tackle preventative measures).

For what concerns the Union, the Directive on attacks against information systems does not contain procedural provisions. In line with the 'fluid' nature of legislation on cybercrime, references to the preventative functions of monitoring are to be found, however, in the Telecom framework (and to a certain extent in the NIS Directive). Article 3 (3) of the open Internet access Directive,[732] as interpreted by BEREC,[733] obliges providers of electronic

[729] Porcedda, Vermeulen and Scheinin (2013).

[730] It should be remembered that such a law should respect parameters of quality specified by the Courts. In the framework of the ECHR, the law must be accessible and respect the rule of law (Shimovolos v. Russia, n. 30194/09, CE:ECHR:2011:0621JUD003019409, para 67). When they do not establish secret measures of surveillance, laws must enable individuals to foresee (Case of Rotaru v. Romania, n. 28341/95, CE:ECHR:2000:0504JUD002834195, para 59.), if need be with appropriate advice, with sufficient precision the consequences produced upon them and thus regulate their conduct. As for the Charter, the ECJ set parameters of quality in *Digital Rights Ireland*, discussed in chapters 6 and 7.

[731] European Commission (2015), *The European Agenda on Security, COM(2015) 185 final*, p. 20.

[732] Regulation 2015/2120/EU of the European Parliament and of the Council of 25 November 2015 Laying down Measures Concerning Open Internet Access and Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services and Regulation (EU) 531/2012 on Roaming on Public Mobile Communications Networks within the Union.

[733] Body of European Regulators for Electronic Communications (BEREC), *BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules* (BoR (16) 127, 2016).

communications to the public to treat all traffic equally (excluding interconnecting traffic and terminal equipment practices). Providers of electronic communications to the public include providers of electronic communications services or networks in the sense of the Framework Directive, and exclude services that are not publicly available. Reasonable traffic management measures are allowed but they cannot, *inter alia*, be based on commercial considerations and monitor the specific content.

Hence, for the sake of exhaustiveness, DPI could not be used for ad-injection and traffic prioritization, or to counter copyright infringement as the ECJ had decided in the *Scarlet Extended*[734] and *Sabam*[735] cases. In both cases, SABAM, a company representing copyright holders, requested and obtained injunction orders against Scarlet Extended (an internet access provider) and Netlog (an online social networking platform), to install a DPI system (Audible Magic[736]) for filtering electronic communications with a view to preventing copyright-infringing file sharing. Both Scarlet and Netlog appealed, and the court decided that the applicable law, construed in the light of fundamental rights, must be interpreted as precluding an injunction made against an internet service provider which requires it to install a preventative system for 'filtering', which applies indiscriminately to all individuals using those services, for an unlimited period of time (and at the expense of either Scarlet or Netlog).

The prohibition of monitoring enshrined in the Internet Access Directive concerns content provided by end-users, such as text, pictures and video, whereas monitoring techniques that rely on the information contained in the IP packet header, and transport layer protocol header (e.g. TCP) are allowed. According to the third subparagraph of article 3 (3) the following are a non-exhaustive list of unreasonable traffic management techniques: block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories. Recital 11 clarifies that "rules against altering the content, applications or services refer to a modification of the content of the communication."

However, the same subparagraph contains three exhaustive exceptions, which must be therefore interpreted strictly, of legitimate aims pursuant to which such unreasonable traffic management techniques can be used, <u>including monitoring as described above</u>, so long as the

[734] *C-70/10 - Scarlet Extended*.
[735] *C-360/10 - Sabam*.
[736] (https://www.audiblemagic.com/). Milton Mueller, Andreas Kuehn and Stephanie Michelle Santoso, 'Policing the Network: Using DPI for Copyright Enforcement' (2012) 9 Surveillance & Society 348; Stefan Kulka and Frederik Zuiderveen Borgesius, 'Filtering for Copyright Enforcement in Europe after the Sabam Cases' (2012) 11 European Intellectual Property Review 54.

processing of personal data is lawful (article 3.4). According to BEREC, all three exceptions "have as common preconditions that the traffic management measure has to be necessary for the achievement of the respective exception ('except as necessary') and that it may be applied "only for as long as necessary".[737] These stem from the principle of proportionality that is well highlighted in the Directive. The first exception, contained in letter (a), is to comply with Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers. The second exception, pursuant to letter (b) is to preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of end-users. The third exception, in accordance with letter (c), is to prevent impending network congestion and mitigate the effects of exceptional or temporary network congestion, provided that equivalent categories of traffic are treated equally.

It should be noted that article 3 of the open access directive seems *prima facie* to respond to the standards of quality established by the Court in *Digital Rights Ireland* (see chapter 1, section 2.3, and chapter 6), and to take in due account rights that have been potentially interfered with, e.g. article 14.

In the following I reason on CIA crimes, content control and surveillance/eavesdropping.

2.3.1 DPI AND CIA CRIMES

DPI combines functionality from intrusion detection/prevention systems and stateful firewalls to detect and block attacks; it does so by checking each packet against known signatures. Attacks such as malware and viruses are illegal data interference, pursuant to article 5 of Directive 2013/40, that can affect industrial secrets and obviously users' personal data and private life. DPI can also block DDOS, worms and spam, which could be said to be illegal system interference pursuant to article 6 of Directive 2013/40 affecting the availability of systems, which is a legal interest of operators and users; spam may be said to be prohibited

[737] Body of European Regulators for Electronic Communications (BEREC) (2016), *Guidelines on net neutrality, BoR (16) 127*, paras 79-80.

(in the context of direct marketing) by article 13 of the e-Privacy Directive (see *supra*, section 1.1, and chapter 3, section 3).

The exception listed in article 3 (3) (b) and possibly (c) may allow the monitoring of content for the sake of cybercrime prevention, thus contributing to that "comprehensive framework of prevention measures accompanying criminal law responses to cybercrime" as stated in recital 2 of the Directive on attacks against information systems. BEREC itself lists threats to security that are the objective of Directive 2013/40: denial of service attacks (illegal interception), spoofing IP addresses (illegal data interference), hacking attacks (illegal access), and recital 14 mentions explicitly cyber attacks occurring as a result of malware (illegal data interference) and identity theft of end users (article 9 of Directive 2013/40) caused by spyware (illegal data interference). This exception would apply to providers of electronic communication to the public, viz. ISPs; hence operators of essential services and of digital services pursuant to the NIS Directive would be automatically excluded. BEREC has left the door open for extending the provisions of the Open Access Directive to internal corporate networks (§ 12) falling in the remit of NIS, though the decision should be taken on a case-by-case basis.

These measures go hand in hand with article 4 (1) of the e-Privacy Directive and article 13 letters (a) and (b) of the Framework Directives, which oblige electronic communications services and public network access providers to employ suitable technical and procedural means to ensure the security of the network and the services issued therein. BEREC is silent about the 'security monitoring systems' used, though for the sake of article 3 (3) (b) such systems may be run continuously in the background (§ 85). It does, instead, claim that specific actions should only be triggered *vis-à-vis* the detection of concrete threats, and provides examples including blocking of IP addresses and internet access services and port numbers (§ 84).[738]

Since malware-oriented DPI can detect and block threats, it both prevents crime and protects personal data and subsequent confidentiality of communications, as recognized by the European Data Protection Supervisor[739] and the Article 29 Data Protection Working Party

[738] This may suggest IP/TCP inspection only, but the report does not provide more details.
[739] European Data Protection Supervisor (EDPS), *Opinion on Net Neutrality, Traffic Management and the Protection of Privacy and Personal Data* (OJ C 34, p 1–17, 2011).

(in the context of email services).[740] These legitimate aims are in line with article 3 (3) (b) and hence justify the interference with privacy rights mentioned *supra*, section 2.2;[741] actually, the interference aims at better protecting the rights, so that it could be argued that the interference is of a positive nature. I should recall, in fact, that preserving the security of personal data constitutes the essence of the right to the protection of personal data as the ECJ stated in *Digital Rights Ireland*. This use of DPI would thus likely be deemed to be permissible, though given the ambiguous remit of NIS, the adoption of a specific piece of law would be desirable for the sake of transparency and accountability.

2.3.2 DPI AND THE FIGHT AGAINST CHILD PORNOGRAPHY

Child pornography is a discomforting topic, as it concerns the most vulnerable members of society, and the citizens of the future. Unsurprisingly, it is an emotionally charged, and at times biased, subject. This makes it an imperative case study of content control, because protection of children is a legitimate aim necessary in a democratic society. The subject has been widely studied elsewhere,[742] and here I only focus on the permissibility of DPI in relation to it.

Child pornography does not concern cyber-security; rather, it is often a horrific business pursued by organized crime online.[743] It is considered an offence by both the Cybercrime Convention (art. 2) and the anti-Child Abuse Directive (chapter 3, section 3.3.3), and subsumes three meanings: a) pseudo child pornography, i.e. images portraying seemingly underage adults (<18) in pornographic poses; b) synthetic child pornography, i.e. the manipulation of pictures of children to simulate scenes of abuse; c) real child pornography, that is the portrayal of an act of abuse on a child.

DPI is said to be a very useful tool to uncover cases of child abuse and pornography and take down rings of (gainful) abusers. Buttressing such claims is fundamental for assessing the

[740] Article 29 Data Protection Working Party, *Opinion 2/2006 on Privacy Issues related to the Provision of Email Screening Services* (00451/06/EN WP 118, 2006).
[741] *Niemietz v. Germany, n. 13710/88*, para 36.
[742] T. J. McIntyre, 'Child Abuse and Cleanfeeds: Assessing Internet Blocking Systems' in Ian Brown (ed), *Research Handbook on Governance of the Internet* (Edward Elgar 2013).
[743] Peter Sommer and Ian Brown, *Reducing Systemic Cybersecurity Risks* (OECD/IFP Project on Future Global Shocks, IFP/WKP/FGS(2011)3 2011) <http://www.oecd.org/governance/risk/46889922.pdf>.

proportionality of the measure, but in order to appraise permissibility, I should start with legality.

To date, there is no legal basis explicitly authorizing the use of DPI engines for the detection of child pornography. As seen in chapter 3 and *supra* (sections 3.3.3 and 1.2.1 respectively), article 25 of the anti-Child Abuse Directive lays down a rule for blocking and taking down content akin to child pornography, but it does not lay down rules (on methods) for detecting pornographic material. The recent trend in drafting memoranda of understanding between police services and private actors with a view to "identifying and removing known child pornography material" and "increasing as much as possible the volume of system data examined,"[744] offers an invalid solution. Memoranda of understanding do not have the force of law. The law authorizing the use of DPI for the detection of child pornography must be adopted at the EU level, as not to do so would hinder the competitive development of the internal market.[745]

Article 3 (3) (a) of the open Access Directive could provide such legal basis, as it enables ISPs to perform monitoring of content "to comply with Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers." Recital 13 of the Directive refers to criminal law requiring blocking of specific content, applications and services, as is the case of the anti-Child Abuse Directive.

Differently from the considerations with respect to article 3 (3) (b), however, BEREC does not state that such measures should be applied on a continuous basis. Requiring service providers to constantly run DPI engines for the sake of cybercrime prevention could infringe the other prohibition of general monitoring laid down by the e-Commerce Directive,[746] whereby member states must not oblige ISPs "to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity", as recalled by the ECJ in *Scarlet Extended* and *Sabam* (*supra*, section 2.3).

---

[744] Global Alliance Partners, *Guiding principles on the Global Alliance against child sexual abuse online. Annex to the Declaration on Launching the Global Alliance against child sexual abuse online* (2012) <http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2012/docs/20121205-declaration-anex_en.pdf>.

[745] Judgment of 10 February 2009 in Ireland v. Parliament and Council, C-301/06, EU:C:2009:68 (Data Retention I).

[746] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), OJ L 178.

It should also be noted that, unlike for CIA cybercrimes, DPI could do nothing to prevent abuse *per se*, but rather it would block the circulation of pictures, and, in an unknown percentage of cases, help identifying perpetrators so that they can be prosecuted. This raises serious issues of public policy and proportionality. Such an objective should be more clearly the purpose of a law adopted with a legal basis in the AFSJ, not the internal market.

In the light of the above, article 3 (3) (a) could be seen as authorizing an ISP to monitor content solely on an occasional basis, to comply with a specific court order. The assessment of permissibility should include a rigorous analysis of the interference with privacy rights. The stakes of the intrusion are very high. The essence of article 7 of the Charter, namely the content of communications, could be interfered with for a potentially large number of users in a way which is not, like in the case of malware prevention, complemented by any tangible benefits. DPI should therefore be deemed impermissible. It should be stressed that in *WebMindLicenses*, relating to proceedings between a legal person, WebMindLicenses, and the Hungarian National Tax and Customs Authority, concerning tax evasion,[747] the ECJ stated that evidence stemming from criminal procedure, and used to take a decision in the context of administrative tax procedure, "obtained and used in breach of the rights guaranteed by EU law and, especially, by the Charter…must be disregarded and the contested decision which is founded on that evidence must be annulled..."[748] Should a Court be of the opinion that the essence is not interfered with, the caveat of necessity and proportionality should be assessed on a case-by-case basis, along the lines of the reasoning in *Digital Rights Ireland* (see *infra*, section 2.4, and chapters 6 and 7). Such a measure would be likely to pass the necessity test only in the case of real, not synthetic, child pornography.[749] In such a case, there would also be conflicting interests concerning the protection of personal data and the private life interest of the children engaged in child pornography.

Hence, currently DPI could be permissible for specific real child pornography investigations only. National laws may need to be revised to comply with article 8 of Directive 2016/680, so as to include at least the objectives and purposes of the processing and the personal data to be processed. Moreover, it should be noted that, pursuant to article 10 therein, human intervention must back up decisions stemming from automated processing. In

[747] The evidence against WebMindLicenses Kft. was obtained in the course of a parallel criminal investigation, not yet concluded at the time of the case, where WML's emails and communications were intercepted without a court order.
[748] *C-419/14 - WebMindLicenses*, paras 87-89.
[749] For an in-depth discussion of the matter, see Akdeniz (2011). See also Perrin v. the United Kindgom, n. 5446/03, CE:ECHR:2005:1018DEC000544603.

my view, the anti-child abuse Directive should be reviewed to include, at a minimum, the same safeguards that the EU legislator requires Member States to adopt. However, DPI is likely to intrude into the essence of at least the right to private life, to the extent that such a measure could be deemed impermissible, which unveils its intrinsic ambiguity. I will come back to this in section 2.4.

2.3.3 DPI AND INTERCEPTION FOR NATIONAL SECURITY

The Snowden Revelations offer an example of how DPI engines can be used to for national security purposes and to tackle serious crime at large, including terrorism, unrelated to Network and Information Security (NIS), posed by 'deviant behaviour'.

For instance, Article 14 of the Budapest Convention allows for extending the scope of application of real-time interception of content data obtained pursuant to article 21 to "other criminal offences committed by means of a computer system, and the collection of evidence in electronic form of a criminal offence," such as 'online terrorism'.[750]

In the Union there is no law that authorizes the continuous and indiscriminate monitoring of content for an undetermined length of time. The invalidated Data Retention Directive[751] prohibited retaining content data, which violates the confidentiality of communications. This prohibition prevented the Directive from being struck down on grounds of violation of the essence of article 7 of the Charter, though it did not save it, either, from the accusation of being disproportionate.

The only reference to intercepting electronic communications is contained in a recital of the Human Trafficking Directive, which makes it an unsuitable legal basis (at the EU level). The proposed counter-terrorism Directive also includes unsuitable formulations, in that they are too vague, such as "counter offences related to terrorist activities when committed through the Internet, including social media" and removing or blocking access to webpages publicly inciting to commit terrorist offences".

[750] United Nations (2012).
[751] Data Retention Directive (2006/24/EC).

These measures would constitute a serious and wide interference with privacy rights, which could engender that feeling of constant surveillance referred to by the ECJ in *Digital Rights Ireland* (§ 37). National provisions should stem directly from – currently absent – provisions of EU law. Moreover, such provisions should first solve the conundrum of the prohibition of general monitoring by ISPs. The reasoning behind the inadmissibility of DPI for continuous child pornography applies, *mutatis mutandis*, to eavesdropping and phishing expeditions. Hence, using DPI engines for phishing expeditions is impermissible as it lacks a legal basis and infringes existing applicable law. The ambiguity, to say the least, of DPI for occasional child pornography applies, *mutatis mutandis*, to eavesdropping and phishing expeditions as well. Any laws should further comply with the minimum requirements set in articles 8 and 10 of Directive 2016/680 illustrated in the previous section (as well as the other provisions of the Directive).

Moreover, the short-term advantages of DPI for serious crime investigation would severely affect not only privacy rights, but also NIS, which is contradictory in two ways.

First, the security of NIS ought to be a crucial national security matter. Landau wrote that the security risks would dwarf the enormous privacy ones.[752] In fact, there would be little incentive to protect the collected information, which could be exploited by both insiders (due to the appeal of big data)[753] and malicious outsiders. After the 2006 AT&T scandal, it emerged that the Narus DPI engine could be configured, once sold, as users saw fit. [754] Infamously, in the 'Athens Affair' CALEA-compliant software sold by Ericsson to Vodafone Greece was used to intercept the government's communications for almost a year before the 2004 Olympic Games.[755] In October 2016 Yahoo was placed under the spotlight as Reuters revealed it had installed a program, on behalf of the US government, to scan incoming emails live for 'selectors' i.e. terms used by a terrorist group.[756] Some weeks before, the company had disclosed a severe breach affecting 500m accounts.[757] Though the link between these two stories has not yet been established, the former chief security officer, who had quit after discovering that such a program was installed, said the scanning program used could have been exploited by hackers. To be sure, the use of DPI engines is not the only example of

[752] Landau (2010), *Surveillance or Security?*
[753] Jaron Lanier, *Who Owns the Future?* (Penguin Books 2013).
[754] Robert Poe, 'The Ultimate Net Monitoring Tool' *Wired* (17 May 2006).
[755] Landau (2010), *Surveillance or Security?*
[756] Jospeh Menn, 'Exclusive: Yahoo Secretly Scanned Customer Emails for U.S. Intelligence Sources' (4 November 2016).
[757] Olivia Solon, 'Yahoo Confirms 'state-sponsored' Hackers Stole Personal Data From 500m Accounts' (23 September 2016).

contradiction:[758] the use of state-sponsored malware is another case in point (e.g. the 'Magic Lantern' and the *Bundestrojaner*).[759]

Second, affecting the confidentiality of communications harms the very rights and privileges that characterise our democracy and that national security should supposedly protect (as discussed in chapters 1 and 2).

2.4 THE AMBIGUITY OF DPI

The outcome of the analysis of the legal permissibility of DPI based on its potential intrusion into privacy rights leads to a paradox, whereby DPI seems both permissible and impermissible.

Running DPI without authorization could constitute an offence: generic online (passive or active) *unauthorized* DPI could amount to illegal interception, i.e. the loss of confidentiality of personal data; active DPI could also amount to system interference, which is the serious hindering of the availability of a computer system. Here, giving up privacy for security would be highly inefficient.

Applicable law seems to support the possibility of running DPI on an *ad hoc* basis for serious crime investigation (including to counter child pornography), but I maintain that *leges speciales* should be revised to include the necessary privacy rights-related safeguards (pursuant to article 62 of Directive 2016/680). Moreover, I believe it to be necessary to address the matter of the potential interference of DPI with privacy rights, and particularly the essence of art. 7 of the Charter (the content of communications).

Applicable law seems to permit running malware-orientated DPI on a continuous basis, provided it is controlled and audited. In fact, private companies may be currently selling DPI as a malware solution, but enabling it to be also used for other purposes,[760] in particular since

[758] David E. Sanger, New York Times, 12 August 2013. Under Einstein, DPI engines already analyse all traffic passing through US governmental networks for security purposes.
[759] Landau 2010. Graham Cluley, NakedSecurity, 9 October 2011; European Digital Rights (Edri), Edri-Gram Newsletter, N. 10.20', 24 October 2012 and n. 11.12, 19 June 2013.
[760] Landau (2010), *Surveillance or Security?*

their business model and the interests of law enforcement officers could converge.[761] BEREC[762] warned that network security could be an excuse to circumvent the prohibition of monitoring (§ 87).[763] Yet, this use of DPI is also not without ambiguity: in order to enforce the security of data and protect confidentiality, DPI interferes with both rights, and in particular the essence of art. 7, viz. the content of communications. This is particularly the case for the latest version of DPI, deep content inspection, which performs the analysis after having re-aggregated the packets, hence on the full 'content'.

Two interrelated reflections ensue. The first is that technology can both enhance and infringe privacy rights, and do so at the same time: for DPI to protect privacy rights, some of the features of those rights must be interfered with. Technology may therefore challenge the complementarity between cybersecurity as NIS/narrow cybercrime prevention and privacy rights found in section 1.

The second reflection is that, in so far as the feature of the right interfered with is its essence, we reach an *impasse*; the use of DPI begs the question of the meaning of interfering with the essence, in this case 'content', a point likely to be decisive for its permissibility. BEREC seems to understand content as what is produced by the end-user: the actual text, or sound. The bar would therefore be very high: only DPI that affects the payload of the application layer would infringe the essence. But what does the ECJ mean by "permit the acquisition of knowledge of the content of the electronic communications"? Is scanning for signatures the acquisition of knowledge? Or is it looking for actual sentences and images? And what about other functions of DPI described in section 2.1 performed on payloads lower than the application level? The payload could still be seen as content, and the metadata it produces (which form part of the notion of correspondence in the ECtHR case law) is as telling as the intelligible content. DPI can severely interfere with the exercise of communications (as in when it silently discards a packet), or their confidentiality (when it replicates/mirrors packets).

This puts the ball in the court of the ECJ. Which test would the court apply? In *Scarlet* and *SABAM*, the ECJ did not perform an assessment of the interference of DPI (called 'filtering') with the right to private life at all, though in § 51 it found that the systematic analysis of all

[761] Bruce Schneier, 'The Vulnerabilities Market and the Future of Security' (2013) <www.schneier.com/crypto-gram-1206.html> accessed 25 June.
[762] Body of European Regulators for Electronic Communications (BEREC) (2016), *Guidelines on net neutrality, BoR (16) 127*.
[763] Bendrath (2011) argued that its use was limited because ISPs could outsource Internet security to users.

content, plus the collection and identification of users' IP addresses (personal data) would constitute an impermissible interference with article 8 of the Charter. Hence, the court condemned both the analysis of content (arguably the signatures used by Audible Magic to recognize digital rights-protected material) and the identification of individuals (which did not require vision of the full content, but IP header only). But there the competing interest was copyright infringement.

Would the court adopt a sweeping bar against (lower forms of) DPI in case of serious (cyber)crime? In *Digital Rights Ireland*, despite acknowledging that metadata "taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them",[764] the ECJ found data retention permissible *prima facie* because it did not affect the content of communications. We can only wonder whether the court would deem signatures, or keywords as permitting "the acquisition of knowledge of the content".

Here we are facing two intertwined issues, at two different levels of abstraction. At the lower level of abstraction, courts do not perform an analysis of technology involved; at a higher level of abstraction, courts do not provide a clear definition of rights, partly because of the 'living instrument' doctrine. While this enables adapting rights to changing times, it creates ambiguity as to their interaction with technology, which requires daring judgments – judgments that fail to materialize (at EU level).

In sum, the ambiguity of DPI results from the fact that the application of standard tests shuns the configuration of DPI engines: different objectives entail the use of different modules, which interfere with privacy rights differently and hence have varying degrees of permissibility. This state of affairs is due to a negative interaction between the facts that: the specifics of technology and possible usage are not subsumed under EU applicable law (viz. technology neutrality); judges do not take responsibility to fill in the vacuum; and the (otherwise welcome) ambiguity of judges in understanding (privacy) rights. These, which in essence form part of my fourth and last hypothesis, are dealt with in the next chapter.

[764] *Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*, para 27.

3 CONCLUDING REMARKS

This chapter led to the validation of hypothesis 1: the trade-off is not a useful explicatory device. The comparison of substantive legal provisions contained in the applicable law to ascertain whether cybersecurity and the rights to private and family life and data protection can be reconciled have borne interesting results.

First, a theoretical convergence is warranted between the prevention of NIS and the rights to the protection of personal data and private and family life. In addition, the case of data/security breaches shows a manifest case of overlap of protection goals (thus confirming hypothesis II).

Second, the trade-off appears to be an inadequate intellectual device (hypothesis I), as it does not capture cases where tackling cybercrime leads to forms of surveillance that may be deemed intrusive into privacy rights that thus harm cybersecurity. This is because the trade-off fails to take into account the pre-eminence of technology in providing *ex ante* and *ex post* solutions in cybersecurity. This has an important bearing on efficiency: trading-off security with privacy may lead to catastrophic results. This raises the important policy question of the coexistence of cybersecurity with SIGINT. Even when there is no complementarity, it would seem possible to reconcile broad cybercrime with privacy rights (hypothesis III). However, a complete response to hypothesis III requires analysing technology, which would also seal the validation of hypothesis II.

To factor in the technological element, I took into account a measure used in connection with NIS and cybercrimes, DPI. However, reliance on applicable law and (scant) case law proved inconclusive. The problem does not reside in the analysis as such, but in a paradigm, that of technology neutrality, because the applicable law does not address the (surveillance) technologies and techniques used for the perpetration, prevention and investigation of offences. The notion of 'technical and organizational measures', mentioned in this chapter and earlier ones, is not accompanied by subsequent clarifications, which courts fail to address. Such an approach negatively interacts with the (otherwise helpful) evolving approach to rights, in what seems to be a circular avoidance of an analysis of the impact of technologies on rights.

Such an impact does not necessarily have to be detrimental, since technologies can play an important role in protecting privacy rights. Ultimately, it is by looking at the impact that such

technologies have on the two rights that one can appraise whether there exists a trade-off between cyber-security and privacy rights. It is to this that I move now, with an open mind: the analysis of technology may subvert the (interim) conclusion that NIS and narrow cybercrime are compatible with privacy rights.

PART 2 - A METHOD TO APPRAISE THE RELATIONSHIP BETWEEN TECHNOLOGY AND PRIVACY RIGHTS

CHAPTER 5 - A METHODOLOGY TO EXPLORE THE IMPACT OF TECHNOLOGIES ON PRIVACY RIGHTS[765]

In the previous chapter I argued that a comparison of substantive legal provisions contained in the applicable law and case law is a necessary but insufficient exercise to ascertain whether privacy rights can be reconciled with cyber-security and thus prove hypotheses II and III. I maintain that this is due to the combined effect of, on the one hand, the paradigm of technology neutrality affecting both law-making and judgments, and on the other hand, the – otherwise beneficial – courts' avoidance of providing strict definitions of rights, in line with the evolving understanding of human rights. I develop this argument, which is my hypothesis IV, in sections 1 and 2.

Section 1 draws lessons from the case study of DPI to demonstrate why legal argumentation based on applicable law and case law is necessary but insufficient to tackle the problem of measuring the impact of technologies on rights. It discusses the negative impact of regulatory technology neutrality and courts' avoidance of appraising technological matters (first part of hypothesis IV).

Privacy scholars have long been confronted with the problem of coping with technologies, not least because, as noted in chapter 4, technology is not only interfering with rights, but also plays an important role in protecting them (e.g. PETs, section 3.5). In recent years, methodologies have been proposed that try to capture, as a side exercise or as the explicit purpose, the impact of technologies on rights. Section 2 discusses the merit and limits of the SurPRISE and SURVEILLE legal approaches as well as privacy impact assessments (PIAs) as a point of departure for the definition of a suitable method. Here, I also highlight the problem of the definitions of rights, whose evasive meaning (influenced by the evolving interpretation of courts) hinders a homogeneous understanding of the impact of technologies on rights (second part of hypothesis IV).

[765] An early draft of this chapter was submitted to the European Commission as Annex F to SURVEILLE Deliverable D 4.10 in February 2015. The draft was not publicly disseminated. Moreover, section 3 of this chapter consists of a substantial revision and extension of the work conducted within Porcedda (2013), *Paper Establishing Classification of Technologies on the Basis of their Intrusiveness into Fundamental Rights* (SURVEILLE Project Deliverable D 2.4).

The analysis of existing methods and their limits calls for a methodology that can bridge law and technology, and which can be derived by creating synergies between literature from different disciplines on the measurement of the impact of technologies on rights and on security. This is the objective of section 3. Based on research conducted in the interdisciplinary project SURVEILLE, I propose a methodology capable of assessing the impact (either synergy or degrees of intrusion) of technologies used in connection to cybersecurity on the fundamental rights to the protection of personal data and respect for private and family life. Note that in this chapter I use cybercrime as an antonym of cybersecurity, for the sake of clarity of exposure. The distinction between narrow/broad cybercrime described in chapter 3 and 4 will be taken up again in chapter 8.

1 BEYOND ARGUMENTATION DERIVED FROM JUDGMENTS AND CASE LAW FOR THE APPRAISAL OF TECHNOLOGY: THE PROBLEM OF TECHNOLOGY NEUTRALITY

The analysis of the legal permissibility of DPI based on applicable law and existing judgments led to a paradox, whereby DPI appeared to be, in principle, both permissible and impermissible. On the one hand, the use of spam and malware-oriented DPI is permissible: the apparent intrusion into privacy rights is geared to safeguard them, as well as NIS. However, appropriate scrutiny should be enabled: engines should focus on malware, spyware and Trojans only.[766] On the other hand, the use of DPI for constant content control is currently impermissible, as it both lacks a legal basis, thus violating the rights to respect for private and family life and the protection of personal data, and imperils cyber-security. The *ad hoc* use of DPI for investigations concerning serious crime could be permissible, provided a specific provision is adopted to ensure the proportionality and transparency of the tool.

I maintain that the paradox results from the fact that the analysis of legal permissibility shuns the configuration of DPI engines and its specific uses, because the specifics of technology and possible usage are not subsumed under EU applicable law. Chandler notes

[766] European Data Protection Supervisor (EDPS) (2011).

that the question as to whether the law is capable of controlling technology is a deeply-rooted cultural as well as legal concern.[767] But in the case of regulation of ICT, the lack of reference to specific tools is the result of an explicit choice, the paradigm of technology neutrality. The product of liberalisation in the market of telecommunications, it purports to strip from laws any references to particular products or services,[768] though the term is far from univocal.[769]

Technology neutrality in the law may be seen as the consequence of a principle as well as a practical concern. As for reasons of principle, the law seeks to be of general application.[770] Therefore, the determination of technological specifications pertains more to different instruments, such as standards. Indeed, according to Reed, two (ambiguous) features underpin the paradigm. The first is online and offline equivalence, i.e. applying rules that produce the same effect, whether technologies are used online or offline. The second is that the laws should not advocate or run counter to a particular technology.[771] As for the practical concern, the legislator is aware that the law develops at a slower pace than technology does. The idea is to foster, or at least not to hinder, the development of new technologies, but also make the law future proof (Koops says 'sustainable'), so as not to require amendment too frequently.[772] Koops identifies an additional practical concern, i.e. steering the development of a technology in a desired direction.[773]

Examples of technology neutrality in legislation can be found in article 17 of Directive 95/46/EC, which lays down that "Member states shall provide that the controller must implement appropriate technical and organisational measures to protect personal data…" Similarly, cognizant of the multiple ways in which an attack can be perpetrated, as well as the rapid pace of development of both software and hardware, recital 16 of Directive 2013/40 on

[767] Jennifer A. Chandler, 'The Autonomy of Technology: Do Courts Control Technology or Do They Just Legitimize its Social Acceptance?' (2007) 27 Bulletin of Science, Technology and Society 339-348. In fact, this could do with the fact that technology embodies the idea of progress, understood as the objective of society, and rooted in science. See Taylor (1989), *Sources of the Self.*
[768] Chris Reed, 'Taking Sides on Technology Neutrality' (2007) 4 Script-ed.
[769] Bert-Jaap Koops, 'Should ICT Regulation be Technology Neutral?' in Bert-Jaap Koops and others (eds), *Starting Points for ICT Regulation* (TMC Asser Press 2005). There, Koops illustrates the inherent ambiguity of neutrality (and ICT, IT and technology), and the different purposes it can pursue.
[770] Reed identified three different legislative techniques. First, technology indifference, which works if the effect of an action or behaviour is unchanged by the simple fact of being committed offline or online. Second, implementation neutrality: regulation that addresses a type of technology (e.g. e-signature), but does not affect its implementation (e.g. the different ways of signing a document electronically). Third, potential neutrality: regulation that clarifies the legal requirements for a certain technology, e.g. the fact that they must all have a certain attribute in order to be legal. Reed (2007). For additional purposes, Koops (2005).
[771] Reed (2007); Koops (2005).
[772] Reed (2007).
[773] Koops (2005).

attacks against information systems reads "this Directive refers to *tools* that can be used in order to commit the offences laid down in this Directive."

The point is that technology neutrality may fail all aims it tries to achieve: making law future-proof; online and offline equivalence; and supporting the development and spreading of a technology.[774] Drafting technology neutral legislation is in fact only feasible if the legislator fully understands the technology and its implications,[775] also for the future, as well as what objective it wants to achieve.[776] Referring to the work of Escudero-Pascual and Hosein on the interception of communications data within the UK Regulation of Investigatory Powers Bill 2000, Reeds observed that "an unsuccessful attempt to achieve technology neutrality has resulted in regulation whose meaning is so vague that its application to the technology is often a matter of guesswork". [777] This is also the case of Directive 95/46/EC, which has not survived the evolution of Web and Internet-related applications, despite its explicit efforts to be neutral.

If the dubious success of technology neutrality at achieving its explicit objectives is a considerable issue, a greater one lies in the fact that tools, technologies and related practices have an increasing bearing on matters of principle, which the law should regulate. Reeds rightly said that "ICT is not an end in itself but is used to achieve commercial and social ends, and it is these that may be changed by technology development in a way which outdates the regulation."[778] Chandler went further and argued that individuals mould their behaviour so as to adapt to novel technologies, which become endowed with seemingly autonomous lives. After revising the many reasons why existing legal institutions may not be able to impose effective controls on technology, Chandler convincingly argued that law (and, in common law countries, judgments) may end up justifying the existence and rationale of technologies, eventually rubber stamping societal approval.[779]

When the law avoids regulating on new matters of principle, not only does the law risk failing to address fundamental societal concerns, but it may also impact on the nature of judgments. If the law does not lay down rules, or refer to specifics of technology, it is less likely that such matters will be used in court as part of the main argument of a case. Some of

[774] Reed (2007).
[775] Ibid.
[776] Koops (2005).
[777] Reeds cites the database Directive as a specific example. Reed (2007), p. 280.
[778] Ibid, p. 282.
[779] Chandler (2007).

the cases discussed in chapter 4 are in point here. The *Digital Rights Ireland* case was acclaimed for its outcome: declaring invalid the Data Retention Directive, which had been the object of much litigation at the national (Romania, Germany, Ireland and Czech Republic[780]) and European level,[781] as well as much criticism by scholarship.[782] However, the *Digital Rights Ireland* case contains a troubling passage:

> *"As regards the question of whether the retention of data is appropriate for attaining the objective pursued by Directive 2006/24, it must be held that, having regard to the growing importance of means of electronic communication, data which must be retained pursuant to that directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive. That assessment cannot be called into question by the fact [...] that there are several methods of electronic communication which do not fall within the scope of Directive 2006/24 or which allow anonymous communication. Whilst, admittedly, that fact is such as to limit the ability of the data retention measure to attain the objective pursued, it is not, however, such as to make that measure inappropriate [...]"*[783]

In this passage the CJEU seems to assess data retention an appropriate measure to attain the aim pursued by the Directive, irrespective of the availability of better, more cost-effective or less intrusive methods. It must be noted that the Data Retention Directive was 'technology neutral': it was silent as to the specifics of the techniques of data retention, leaving the matter entirely in the hands of Member States (and judges). The *Scarlet* and *SABAM* judgments were similarly acclaimed for their protection of fundamental rights *vis-à-vis* the enforcement of (technology neutral) digital rights management. Yet, even if the ECJ was pronouncing itself on the use of DPI, it never mentioned it explicitly, let alone the specific engine used, referring instead to a 'filtering system', speaking of which, it said "it is common ground that its

[780] I discussed these judgments in Porcedda, Vermeulen and Scheinin (2013), section 3.4.2.
[781] *C-301/06 - Ireland v. Parliament and Council (Data Retention I). Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*.
[782] Among others, see Tuomas Ojanen, 'Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance. Case Note on Court of Justice of the European Union, Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others' (2014) 10 European Constitutional Law Review 528–541.
[783] *Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*, paras 49-50.

implementation of that filtering system would require…active observation of all electronic communications conducted on the network of the ISP"[784] (§ 39-40).

The problem may be that tackling technological innovations in case law requires considerable technical expertise. In fact, Grabowski and Chandler[785] noted that courts may have an aversion to delving into technology irrespective of the characteristics of law, primarily because of the lack of technical knowledge. Further examples could be offered by the biometric passport cases, *Schwarz*[786] and *Willems.*[787] In the first case, Mr Schwarz filed an action against the *Stadt Bochum* after the latter refused to issue a passport, because Mr Schwarz denied providing his fingerprints. As for the second, the applicants were refused passports because they declined to provide their biometric data (fingerprints and facial image) alleging the potential infringement of their private life and personal data protection, particularly in the light of the fact that the data would be stored on three different media, and the absence of guarantees that the data so collected would not be used for different purposes. In *Schwarz*, at § 41, the ECJ held that "*it is common ground* that the storage of fingerprints on a highly secure storage medium as provided for by that provision requires sophisticated technology. Therefore such storage is likely to reduce the risk of passports being falsified and to facilitate the work of the authorities responsible for checking the authenticity of passports at EU borders." The Court dismissed reference to errors of implementation: the "fact that the method is not wholly reliable is not decisive. Although that method does not prevent all unauthorised persons from being accepted, it is enough that it significantly reduces the likelihood of such acceptance that would exist if that method were not used" (§ 43).s

When referring to iris scans, seen as "the only real alternative to the taking of fingerprints raised in the course of the proceedings before the Court" (§ 51), the Court did not engage in an analysis of the functioning of the technique, but simply stated it "is not yet as advanced as fingerprint-recognition technology" and finds it unsuitable for general use on grounds of costs, being "significantly more expensive than the procedure for comparing fingerprints" (§ 52). The Court did not delve into any further analysis, but rather lifted itself from further responsibility, because "nothing in the case file submitted to the Court suggests that (an iris scan) would interfere less" (§ 51) and "the court has not been made aware of any (alternative)

[784] *C-70/10 - Scarlet Extended*.
[785] Mark Grabowski, 'Are Technical Difficulties at the Supreme Court Causing a "Disregard of Duty"?' (2011) Journal of Law, Technology & Internet 93-112. Chandler Chandler (2007). Brian Fung, 'The Aereo Case is Being Decided by People who Call iCloud 'the iCloud.' Yes, Really' *The Washington Post* (13 April 2014).
[786] Judgment of 17 October 2013 in Schwarz, C-291/12, EU:C:2013:670.C-291/12.
[787] Judgment of 16 April 2015 in Willems, Joined Cases C-446/12 to C-449/12, EU:C:2015:238.

measures". The reader may find here a timid request to submit better evidence, an interpretation which is frustrated by the subsequent case *Willems* (and the abovementioned *Digital Rights Ireland*), which follows the reasoning developed in *Schwarz*.

Whether or not the lack of technical knowledge is the real reason for courts' aversion to delving into technology, such aversion carries serious risks. Grabowski described such risks in terms of undermining the effectiveness and relevance of the role of courts;[788] the potential unwillingness of affected parties to submit important cases for judicial review;[789] the danger that important cases could be disregarded by the Courts, despite the relevant social questions they raise; and even worse, a disregard of duty by the court. Quoting US Supreme Court Justice Scalia in *Ontario v. Quon*:

> *"Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice. The Court's implication…that where electronic privacy is concerned we should decide less than we otherwise would (that is, less than the principle of law necessary to resolve the case and guide private action)—or that we should hedge our bets by concocting case-specific standards or issuing opaque opinions—is in my view indefensible. The-times-they-are-a-changin' is a feeble excuse for disregard of duty."*[790]

What kind of conclusions could be drawn from this discussion? One, which will be investigated later in this thesis (chapter 8 and conclusions), is that the legislator should seriously consider whether technology neutrality represents the best regulatory option in the light of the objectives it wishes to achieve.[791] In certain circumstances, different choices, such as technology specificity, may be better. Reeds argued that technology specific law may be beneficial in terms of legal certainty, reduced costs of compliance, increased compliance, avoidance of spill-over of legislation to other unforeseen areas, as well as the ease with which regulation can be kept up to date by means of regular reviews (an example where this has been possible without causing any disruptions was the automotive industry).[792]

---

[788] Quoting Judge Shelton, Grabowski (2011).
[789] Ibid.
[790] Concurring opinionof Judge Scalia in the case of City of Ontario, California, et al. V. Quon et al. Supreme Court Of The United States, Syllabus Certiorari To The United States Court Of Appeals For The Ninth Circuit, No. 08–1332, 17 June 2010, 25.
[791] Technology neutrality may be desirable in certain circumstances. In general, Koops (2005). With reference to criminal law, Flanagan (2005).
[792] Chris Reed, Taking Sides on Technology Neutrality, Script-ed, Volume 4, Issue 3, September 2007.

Second, even if judgments are affected by the same fallacies suffered by hard regulation of technology (i.e. they are retroactive, often coming into effect when the technology has evolved), courts should urgently address matters of law to avert the risks described by Grabowski and sanctioned by Justice Scalia. In fact, and to be sure, one cannot do without an analysis of judicial decisions, which set the criteria to identify interference, or else the respect, protection and fulfilment of rights in concrete circumstances.

Rather, and as the third most important conclusion of this analysis, one should appreciate the limitations of existing judgments in providing sufficient answers for the object of this enquiry, also bearing in mind that not all cybercrimes, let alone the technologies used to perpetrate, prevent and investigate them, have undergone a process of judicial appraisal.[793] In the case of judgments issued by the CJEU and the ECtHR,[794] an additional element to take into account is the constraints flowing from the institutional settings in which the two courts operate.[795]

I now move onto reviewing recent scholarly attempts to factor the impact of technology into human rights assessment.

2 IN SEARCH OF A METHOD TO MEASURE THE IMPACT OF TECHNOLOGIES ON RIGHTS

This section discusses existing methods to legally appraise the impact of technology on (privacy) rights: the SURVEILLE project method, the SurPRISE project method and privacy impact assessments. All these methods have several merits and provide an important framework for assessing and framing the relationship between security and rights.

[793] Moreover, the CJEU (as explained in chapter 1) did not have competence in judging matters within the AFSJ until 2009; no case concerning NIS-related cybercrimes has been brought before it.

[794] Jonas Christoffersen and Mikael Rask Madsen (eds), *The European Court of Human Rights between law and politics,* edited by *Jonas Christoffersen and Mikael Rask Madsen* (Oxford University Press 2011).

[795] Maurice Adams and others (eds), *Judging Europe's Judges. The legitimacy of the case law of the European Court of Justice* (Hart Publishing 2013). It should also be mentioned that some commentators stress the Court's cryptic and at times oracular interpretive style. In general, see ibid. In particular, see the contribution by Joseph H. H. Weiler, 'Epilogue: Judging the Judges - Apology and Critique' in Maurice Adams and others (eds), *Judging Europe's Judges. The legitimacy of the case law of the European Court of Justice* (Hart Publishing 2013).

Nevertheless, I argue that these methods fail in providing the granularity needed to address the relationship between cybersecurity and privacy rights, which paves the way to the method proposed in section 3.

2.1 THE SURVEILLE AND SURPRISE METHODOLOGIES

The SURVEILLE and SurPRISE projects, of which this thesis is an expression, proposed a method of solving two related issues: assessing the relative impact of surveillance technologies on fundamental rights; and determining an algorithm to choose between different permissible technologies. To do so, they relied on the integration of a rigorous test for permissible limitations and the core-periphery model, which I turn to next. The analysis of the modified test for permissible limitations is followed by a presentation of the SURVEILLE and SurPRISE methods, and a discussion of their merits and limitations in relation to this enquiry.

2.1.1 THE TEST FOR PERMISSIBLE LIMITATIONS AUGMENTED BY THE CORE-PERIPHERY MODEL

Classic legal analysis investigates interference into rights by applying a balancing or proportionality test. For the legal theorist Alexy, there are two possible ways of construing constitutional rights, which he labels 'narrow and strict', and 'broad and comprehensive'. In the former, rights are understood simply as legal rules, and are applicable like any other legal rule within a legal system.[796] In the latter, which he favours, rights are seen as principles and have pride of place in a legal system. In particular, constitutional rights have the character of values as well as principles (chapter 1, sections 2.1-2.3), both having force *vis-à-vis* the entirety of the legal system. However, both values and principles tend to collide, which requires mechanisms to adjudicate the collision. Whatever the nature of the interferences into a qualified right (whether caused by a right or a legitimate interest in a democratic society),

[796] Alexy (2008).

courts evaluate their permissibility by means of tests derived from case law and applicable legal instruments (*infra*, section 3.4).

A crucial technique of adjudication is the proportionality test, composed of an assessment of suitability, necessity and proportionality. Alexy[797] refers to the latter as balancing, which is the fundamental technique to resolve a collision of principles. It consists of the following steps: determining the degree of importance of the interfered principle, by weighing the seriousness of the interference with the first principle; assessing the importance of satisfying the competing principle causing the interference; and resolving the relational clash, by appraising whether satisfying the competing principle justifies an interference with the first.[798] Such collisions are resolvable because principles are commensurable, since the term of reference is the Constitution, and because of the availability of scales (*infra*, section 2.1.2).

A pure application of balancing, however, could lead to a stalemate, for instance when two equally important principles collide, and their relational interference is equally serious (*infra*, section 2.1.2). Moreover, although judicial decisions are informed by uniform legal principles, the weight applied to each principle often depends on the right at stake. Such a clash of principles can only be solved by elevating one set of values above another, with the consequence of engendering a reductionist view of rights that unjustly sacrifices the idea of their classic interrelatedness.[799] The addition of 'nuances' to a pure application of balancing allows for the avoidance of a reductionist view of rights; this is the case of the essential and inviolable 'core' anticipated in chapter 1 (sections 2.2 and 2.3.1). The idea that any human right contains an essential and inviolable 'core' stems from a combined reading of article 52 of the Charter, the case law and general comments by the Human Rights Committee (hereafter HRC), and a reinterpretation of Alexy's theory of rights.[800] As Scheinin wrote:

> *"[...] The theory can be applied to explain how any fundamental right would have an inviolable core (or more than one such core) sealed in a rule, and a periphery surrounding that core and subject to permissible limitations*[801] *"*[802]

[797] Robert Alexy (2008), 'Constitutional Rights and Legal Systems'.
[798] Alexy (2008), 'Constitutional Rights and Legal Systems'.
[799] United Nations, International Human Rights Instruments, *Report on Indicators for Monitoring Compliance with International Human Rights Instruments* (HRI/MC/2006/7, 2006), 3.
[800] Scheinin (2009), *Terrorism and the Pull of 'Balancing'*. See at Alexy (2008), 'Constitutional Rights and Legal Systems'.
[801] See also Postscript in Alexy (1992; 1994; 2008).
[802] As formulated by Martin Scheinin and the EUI team in Kreissl and others (2013), p. 14.

As for the EU fundamental rights doctrine, article 52 of the Charter[803] refers to the inviolability of the essence of fundamental rights. Likewise, one of the questions of the test or 'checklist' elaborated by the Commission to assess the compliance of legislation with the Charter reads: "would any limitation preserve the essence of the fundamental rights concerned?" Moreover, the HRC declared in the context of several opinions that restrictions on rights must not intrude upon the 'essence' of a human right.[804] However, the idea of a core is proposed as a metaphor, in that fundamental rights may hold multiple cores, and,

> *"Speaking of an 'essence' or a 'core' should not be seen as preventing contextual assessment, as the essence or core can be defined through a multitude of factors."*[805]

2.1.2 THE SURVEILLE SCORING METHOD

The SURVEILLE methodology of assessment of intrusion into fundamental rights is based on the application of nuanced balancing, i.e. proportionality nuanced by the core-periphery approach just discussed, and takes inspiration from Alexy's suggestion of using a scale to perform balancing. The use of scales allows to appraise the commensurability of a principle with another: "the question is not the direct comparability of some entities (i.e. of comparable facts), but the comparability of their importance for the constitution, which of course leads indirectly to their commensurability".[806] To develop the scale to perform balancing, Alexy takes inspiration from the Titanic case (BVerfGE 86), which deals with the clash between freedom of expression and personality rights, and consists in the following steps. First, assessing the intensity of the interference with the first principle: light, moderate, serious (and even very serious or extraordinary). Second, establishing the degree of the importance (or permissibility) of the interference, which is based on a similar scale, applied *a contrario*: how would the competing principle be affected if it did not interfere with the first principle?

---

[803] Charter, art. 52.1.

[804] Human Rights Committee (1999). Human Rights Committee, *General Comment n. 27. Freedom of Movement (Article 12)* (CCPR/C/21/Rev1/Add9, 1999); Human Rights Committee, *General Comment n. 31, The Nature of the General Legal Obligation* (2004); Human Rights Committee, *General Comment No. 32. Article 14: Right to Equality Before Courts and Tribunals and to a Fair Trial* (CCPR/C/GC/32, 2007); Human Rights Committee, *General Comment n. 34. Article 19: Freedoms of Opinion and Expression* (CCPR/C/GC/34, 2011); Porcedda, Vermeulen and Scheinin (2013).

[805] See Scheinin in Porcedda, Vermeulen and Scheinin (2013), pp. 43-44.

[806] Alexy (2008), 'Constitutional Rights and Legal Systems', p. 12.

The SURVEILLE scale tries to measure the importance of a right interfered with by a particular use of a technology, and the level of intrusion within that right, which correspond to Alexy's scale, by using grades or scores: 1 means light, 2 means serious, and 4 means high. Thus, "(a) score of '1' represents a low, '2' a medium and '4' a high relative weighting of the fundamental right. A score of '1' represents a low, '2' a medium and '4' a high (or serious) level of intrusion into that right."[807] The scores are then multiplied with each other (importance * interference). Results vary from the lowest level of intrusion, scoring ½ (as explained in the next paragraph), and the highest level of intrusion, scoring 16. However, the highest threshold of permissibility is set at 9. A score of 10 would equal an impermissible intrusion into a fundamental right. "The rationale lies in the comparison between the usability and fundamental rights score. Accordingly, even the highest usability score, which weighs 10, cannot legitimise the intrusion into a fundamental right weighing more than 10. When the usability score is lower than 10, any fundamental rights intrusion above that score also indicates an impermissible measure."[808]

Two further caveats apply. First, any intrusion into fundamental rights, even where the score is low, would be deemed impermissible if there was either no legal basis or an inappropriate one, i.e. lacking the requirements of clarity and precision. Since the analysis is conducted in the abstract, i.e. considered independently from a particular jurisdiction, the potential legal uncertainty is compensated for by multiplying the result of the score [(importance * interference) * reliability of the law]. "The scale is as follows: ½ is the lowest value indicating the understanding of a lay person; ¾, is a medium value resulting from the agreement within the expert team, in the absence of clear case law; and 1 is the highest value, deriving from the assessment of the expert team supported by reference to clear case law."[809] Such a potential risk is further compensated for by the fact that the assessment is based on a scenario specifying the use of each technology. A second caveat is that the potential addition of a judicial authorization would reduce all fundamental rights intrusion scores by a multiplier of 3/4.

The methodology, developed in deliverable D 2.6,[810] can be best illustrated by means of a concrete example. Table 6 below shows the considerations on the permissibility of the

[807] Martin Scheinin in Scheinin and others (2013), p. 1.
[808] Martin Scheinin in ibid.
[809] Martin Scheinin, in ibid.
[810] John Guelke and others, *Matrix of Surveillance Technologies* (SURVEILLE Project, Deliverable D 2.6 2013).

PredPol system, based on work of mine within the SURVEILLE project.[811] The first row describes the use of the technology within the given scenario. The assessment results from the combined scores attributed to the importance of the right, the degree of intrusion into it, the relevant case law and certainty of law. The results are inserted into a matrix that visually summarizes the assessment. The total scores suggest that the PredPol system is permissible, and the intrusions proportionate and such as not to affect core areas of each right.

Surveillance technology: The PredPol system			
"… The PredPol system predicts a higher likelihood of further car radio thefts in certain streets of Wysteria, and on this basis the decision is taken to deploy additional police to the area to look out for this type of crime. Bill…is walking through Wysteria on his way to the city centre and stops when he hears the sound of breaking glass. He turns around and sees a parked car with a broken window. While looking into the car a deployed police officer, sent to the street on the basis of the PredPol data, arrives. The police officer sees Bill with his hand in the window of a car, whilst the car's radio is still in place in the vehicle. The police officer arrests him on suspicion of attempted theft."			
Affected individuals	**a) All individuals in the targeted area and b) Bill in particular**		
Fundamental right	**Privacy**	**Data protection**	**Other fundamental rights: Non discrimination**
Importance of the right	Interferes with periphery of the right to privacy due to the increased police presence (1)	No personal data of victims, offenders, or law enforcement is collected. Right to the protection of personal data does not apply.	Non-discrimination, 1 "periphery" because it could lead to control more tightly people residing in poor and segregated neighbourhoods, where crime rates are higher, to be exposed to tighter controls. Predpol may also lead to subconscious de facto profiling based on ethnicity.
	Score: 1	***Score: 0***	***Score: 1***
Degree of intrusion	Intrusion is weak (1) since the Predpol system influences privacy only indirectly.	No intrusion	Weak (1) since the argument concerning the possible profiling is merely a presumption and can be countered by proper training of the police force.
	Score: 1	***Score: 0***	***Score: 1***
Relevant case law / certainty of law	No case law strictly applicable	Not relevant	No case law strictly applicable
	Score: 3/4	***Score: 0***	***Score: 3/4***
Total Score	**3/4**	**0**	**3/4**

Table 6 Fundamental Rights Intrusion Assessment in relation to the PredPol system[812]

[811] Michelle Cayford and others, *Consolidated Survey of Surveillance Technologies* (SURVEILLE Project Deliverable D 2.9 2015).
[812] The assessment was refined by Tuomas Ojanen, Jhua Lavapuro and Martin Scheinin in the annex to ibid.

2.1.3 THE SURPRISE EARLY ASSESSMENT ALGORITHM

Within the SurPRISE project, the use of a nuanced balancing, i.e. proportionality nuanced by the core-periphery approach discussed above, was instead used to develop an algorithm to perform an early assessment of a proposed solution (or SOST) to a security problem,[813] rather than one carried out at the endpoint of the policy flow. Such an algorithm could combine compliance with (privacy) rights and the needs of law enforcement agencies when conducting an investigation (in a more general fashion, of privacy and security).

The test, elaborated by Scheinin[814] and illustrated in section 3.4 below, reads as follows. For each threat requiring a solution 'necessary in a democratic society', there exist multiple solutions (A, B, C, and D). The first step consists in appraising the effectiveness of the technology, or answering the question "does it work?" In the model, since D does not work in actually producing better security, it should be excluded. Therefore, the second step consists in appraising whether A, B, and C violate the core or otherwise go beyond the permissible limitations of privacy. In our illustration, we imagine that A does not pass the test for permissible limitations, and should thus be excluded. The final choice between solution B and C depends on a proportionality assessment.

It is not self-evident that the more efficient solution B should be selected, if, at the same time, it is much more intrusive into privacy than its alternative C is. If a clearly greater protection of privacy can be achieved through C, and if simultaneously a level of security close to that guaranteed by B can be reached, or even exactly the same degree of security at a minimally higher (financial) cost, then C should be selected. If, on the other hand, B provides for a much higher degree of security than C, then an effort should be made to reduce B's intrusiveness into privacy rights (i.e. in-built Privacy by Design, security features, data quality features etc.), and one is allowed to choose B, while ensuring that after the modifications the privacy intrusion is proportionate to the security benefit obtained.

[813] Kreissl and others (2013).
[814] Scheinin and Porcedda in ibid, p. 14.

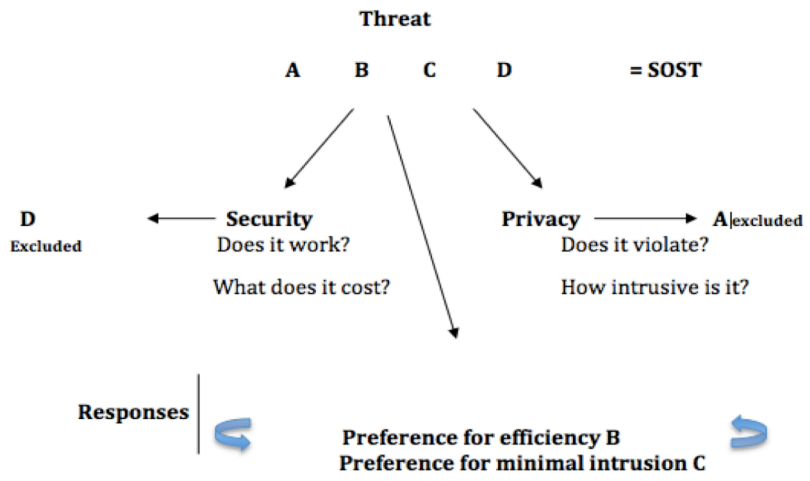


Figure 3 SurPRISE test for early assessment of security solutions

2.1.4 Merits and limitations of core-periphery and the SURVEILLE and SurPRISE methods of assessment

On top of technology neutrality, an additional problem of classic legal analysis in appraising the impact of technologies on privacy rights is that courts have constantly avoided providing a firm definition of the content of both rights (chapter 5, section 2.2.3). While this leaves the door open to an evolving interpretation of both rights, it also hinders the practical assessment of the threshold of permissibility of limitations to rights outside of the courtroom. The test for permissible limitations enriched by the core-periphery method allows establishing clearer thresholds of intrusions, thus avoiding a (wrongly) reductionist approach to fundamental rights. This is an important contribution to the attempt to establish the relationship between a security measure and a fundamental right.

The SURVEILLE scoring method, in particular, could be used to assess the permissibility of a technology, while the SurPRISE methodology could provide a policy to discriminate between different technologies.

It has to be considered, however, that understanding the exact content of rights is a preliminary step to identifying the core. The test for permissible limitations does not provide

guidance on how to define the content of the rights under analysis; the SURVEILLE scoring method also lacks a clear definition of the content and cores of rights.

Moreover, both methods rely on a superficial understanding of technology. Even if the SURVEILLE method integrates ethical, technological and legal considerations into a single decision support system,[815] each analysis is conducted independently. The legal analysis did not build on an in-depth understanding of technology, nor did technologists sit with lawyers to understand each other's needs. In the following section I present the last method, PIAs.

2.2 PRIVACY IMPACT ASSESSMENTS (PIAS)

Privacy Impact Assessments (hereafter PIAs) are instruments used to perform an analysis of the possible impacts on privacy rights of certain measures or technologies, checking compliance with applicable law and proposing how to mitigate possible negative effects.[816] PIAs are variably described as a process whereby both "the potential impacts and implications of proposals that involve potential privacy invasiveness are surfaced and examined,"[817] and "a conscious and systematic effort is made to assess the privacy impacts of options that may be open in regard to a proposal", and "an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated."[818]

Rooted in the experiments performed in the context of environmental policies, PIAs are an expression of the increasing use in policy-making of technology assessments, cost/benefit analyses, impact statements and impact assessments.[819] Wright and others[820] suggest PIAs

[815] See Martin Scheinin and Tom Sorell, *Synthesis Report from WP4, merging the ethics and law analysis and discussing their outcomes* (SURVEILLE Project Deliverable D 2.10 2015).
[816] Paul De Hert and David Wright, *Privacy Impact Assessment* (Springer 2012).
[817] Roger Clarke, 'Privacy Impact Assessments', Xamax Consultancy Pty Ltd, February 1998, at http://www.rogerclarke.com/DV/PIA.html in Roger Clarke, 'PIA Origins and Development' (2009) 25 Computer Law & Security Review 123-135.
[818] B. Stewart, 'Privacy impact assessments' Privacy Law & Policy Reporter 3, 4 (July 1996) 61-64, at <http://www.austlii.edu.au/cgi-bin/disp.pl/au/journals/PLPR/1996/39.html> in ibid.
[819] According to Roger Clarke, the increasing adoption of PIAs is either due to a late reaction of the public sector to the outcry sparked by privacy-invasive initiatives of governments and corporations, or it is part of the wider trend towards risk management, where the burden of proof is placed on the proposers of projects who realized that privacy is an important factor in determining the wide adoption of proposed projects. Ibid. See also David Parker, '(Regulatory) Impact Assessment and Better Regulation' in Paul de Hert and David Wright (eds), *Privacy Impact Assessment* (Springer 2012).

could be used to give substance to the precautionary principle[821] established by the CJEU in the context of BSE (mad cow disease):

> *"Where there is uncertainty as to the existence or extent of risks to human health, the institutions may take protective measures without having to wait until the reality and seriousness of those risks become fully apparent."*[822]

In other words, PIAs enable the assessment of potential issues before they emerge and pose risks to rights and values, and may therefore act as an "early warning system", and thus a necessary aspect of due diligence exercises, in combination with the trend towards privacy by design (hereafter PbD).[823]

Wright and Raab[824] suggested that PIAs could be a useful instrument to check the impact of either a measure or technology interfering with privacy rights (as well as other societal values), and performing surveillance in general. The authors understand surveillance as a set of processes including, but not limited to, the literal meaning of "watching". Surveillance encompasses the processes of listening, locating, detecting, *dataveillance*, and the assemblages of two or more of those functions.[825] It can be performed by the public sector, the private sector and society. It is therefore relevant to appraise the extent to which PIAs can help assess whether privacy rights can be reconciled with the pursuit of cybersecurity, particularly taking into account measures of investigation and analysis, as discussed in chapter 4.

---

[820] David Wright and others, 'Minimizing Technology Risks with PIAs, Precaution, and Participation' (2011) 30 IEEE Technology and Society Magazine 47.

[821] An academic definition is provided by R. von Schomberg: "Where, following an assessment of available scientific information, there are reasonable grounds for concern for the possibility of adverse effects but scientific uncertainty persists, provisional risk management measures… may be adopted… without having to wait until the reality and seriousness of those adverse effects become fully apparent". R. von Schomberg, "The Precautionary Principle and its normative challenges," in Implementing the Precautionary Principle: Perspectives and Prospects, E. Fisher, J. S. Jones and R. von Schomberg, Eds., Cheltenham, U.K. and Northampton, MA: Edward Elgar, 2006, pp. 19–41. Quoted in ibid, 48.

[822] Judgment of 5 May 1998 in United Kingdom v. Commission, C-180/96, EU:C:1998:192, para 63.

[823] PIAs are not a part of the tenets of PbD introduced by Ann Cavoukian, but can lead towards PbD if properly designed. Ann Cavoukian, *Privacy by Design in Law, Policy and Practice. A White Paper for Regulators, Decision-makers and Policy-makers* (Information and Privacy Commissioner, Ontario 2011).

[824] Charles Raab and David Wright, 'Surveillance: Extending the Limits of Privacy Impact Assessments' in Paul De Hert and David Wright (eds), *Privacy Impact Assessment* (Springer 2012).

[825] Ibid.

2.2.1 *How PIAs work and their 'hard law' appeal*

PIAs consist in articulated questionnaires that allow for evaluating several elements of a measure or project. Based on the systematization of various existing definitions, Roger Clarke identified nine features of PIAs.[826] PIAs are not privacy policies or strategies, but are (i) "performed on a project or initiative"; PIAs are different from audits, because they are (ii) "anticipatory in nature", they are checks made before the start of a project; (iii) PIAs have a "broad scope in relation to the dimensions of privacy", in that they do not only assess personal data protection, but also privacy in its several dimensions (at least in the Australian PIAs developed by Clarke). PIAs are more comprehensive than a cost/benefit analysis, risk assessment, or compliance assessment, because they encompass all (iv) "perspectives reflected in the process" and (v) "the expectations against which privacy impacts are compared" by taking into account the participation of stakeholders; (vi) PIAs identify problems and try to find solutions; they are both a (vii) process and a (viii) methodology; finally, (ix) PIAs require high level involvement and approval, or "intellectual engagement from executives and senior managers".

Importantly for the objective of this thesis, De Hert[827] proposed performing two separate assessments for 'privacy' and 'data protection'. However, personal data protection assessments would merely be compliance checks with the applicable binding law. An assessment of the protection of personal data should evaluate respect for the principles of legitimacy, purpose restriction, security and confidentiality, transparency, the data subject's participation, and accountability. These, in practice, correspond to fair information principles (see chapter 2 section 3.3.2, and chapter 7).

Concerning the right to private and family life, De Hert rightly points to the fact that the ECtHR has avoided defining clearly the scope of the right to privacy under the doctrines of the "living instrument" and "practicality and effectiveness", and the CJEU has followed suit. As a result, however, the impact on privacy of a technology should be evaluated with an ideal test for permissible limitations as developed by international courts and synthesized by Scheinin:[828] (1) the technology should be used in accordance with and as provided by the law;

[826] Clarke (2009), 'PIA Origins and Development'.
[827] Paul De Hert, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments' in Paul De Hert and David Wright (eds), *Privacy Impact Assessment* (Springer 2012).
[828] Ibid. Though De Hert does not explicitly attribute the origins of Scheinin's earlier work, which can be found in Scheinin (2009), *Report on Human Rights and Fundamental Freedoms while Countering Terrorism*, paragraph 17. The references are systematized from General Comment No. 27 by the Human Rights Committee,

(2) the technology or processing must serve a legitimate aim; (3) the technology should not violate the core aspects of privacy rights; (4) the technology should be necessary in a democratic society; (5) the technology should not have or give unfettered discretion; (6) the technology should be appropriate, least intrusive and proportionate; (7) the technology should not only respect privacy requirements but also be consistent with other human rights."[829] The test for permissible limitations is discussed in greater detail *infra*, section 3.4.

PIAs are not exempt from shortcomings, varying from the circumstances in which they are introduced, to the regulatory obligations, to the political will and oversight surrounding them,[830] but they are generally seen as advantageous instruments, both for the public and the private sector, in managing risks upfront. Further, they derive benefits in terms of gaining trust, improving image and reducing liability. Lawmakers have increasingly expressed their interest, and the potential force of law gives PIAs a strong appeal for the sake of evaluating the impact of technologies on rights. The General Data Protection Regulation (hereafter GDPR)[831] contains provisions on *data protection* impact assessments. Article 35 (1) mandates data processing likely to result in a high risk to the rights and freedoms of natural persons, in particular using new technologies to be preceded by an assessment of the impact of the envisaged processing operations on the protection of personal data. Even if measures already in force do not explicitly mandate the execution of PIAs,[832] obligations pointing in that direction already exist: prior checking[833] and prior consultation, two procedures mandated by article 20 and 28 respectively of Directive 95/46/EC (and envisaged also by Convention 108[834]). The use of PIAs was formally endorsed by the International Conference of Data Protection and Privacy Commissioners in 2009. Section 22, paragraph (f) of the Madrid Resolution[835] recommends the adoption of PIAs as a proactive measure to promote better

---

Human Rights Committee (1999), *General Comment n. 27*. See also Scheinin (2009), *Terrorism and the Pull of 'Balancing'*. Scheinin and Vermeulen (2011), 41. Porcedda, Vermeulen and Scheinin (2013).

[829] De Hert (2012).

[830] For an in-depth analysis of the advantages and disadvantages of PIAs, see the various chapters reporting practical experiences on PIAs in De Hert and Wright (2012).

[831] General Data Protection Regulation (2016/679/EU).

[832] David Wright and others, *A Privacy Impact Assessment Framework for Data Protection and Privacy Rights. PIAF Project Deliverable D1* (Report Prepared for the European Commission, Directorate General Justice, 2011).

[833] Prior checking differs from PIAs in that the latter is facultative and performed by the data controller, rather than the DPA, but the two may be seen as complementary. Guendal Le Grand and Emilie Barrau, 'Prior Checking' in Paul De Hert and David Wright (eds), *Privacy Impact Assessment* (Springer 2012).

[834] Wright and others (2011).

[835] International Conference of Data Protection and Privacy Commissioners, *Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data (The Madrid Resolution)* (30th International Conference of Data Protection and Privacy Commissioners 2009).

compliance with the regulatory framework.[836] Finally, a strong soft law proposal for the implementation of PIAs is also contained in the 2009 RFID Recommendation.[837]

2.2.2 *Merits and limitations of PIAs (for this enquiry)*

PIAs have several merits, but there does not seem to be a standard methodology to carry PIAs out. Each PIA is an instrument tailored to the specific features of the system under analysis. Examples include the ADVISE project,[838] which used PIAs to build a smart CCTV system respectful of privacy rights. Another proposal consists in structuring PIAs around the principles of privacy by design (the two concepts being separate),[839] whereby the questionnaire could revolve around the seven principles of PbD and their sub-dimensions.[840] The suggestion to use PIAs as tools to assess the potential interference of systems and technologies with rights and values from the perspective of surveillance has not been accompanied by concrete proposals.

What is required is a method that compares systems and technologies against surveillance functions. At the same time, there should be a uniform understanding of the scope of the rights analysed. Roger Clarke argues that Australian PIAs are based on a standard understanding of the scope of privacy (based on the categorization he developed throughout the years), and the proposal for a PIA compliant with PbD suggests including a glossary explaining the meaning of privacy. But this is by no means an established feature;[841] the examples analysed earlier in this section do not contain workable definitions of the two rights. De Hert, for instance, suggests ignoring the scope of the rights and focusing on assessing the technologies based on their compliance with a test for permissible limitations. The test for

[836] For a discussion of the importance of PIAs in the Madrid Declaration, see Artemi Lombarte Rallo, 'The Madrid Resolution and the prospect for a transnational PIAs' in Paul De Hert and David Wright (eds), *Privacy Impact Assessment* (Springer 2012).
[837] Wright and others (2011).
[838] ADVISE is a project financed by the Seventh Framework Programme. Project website: http://www.advise-project.eu.
[839] Pat Jeselon and Anita Fineberg, *A Foundational Framework for a Privacy by Design Privacy Impact Assessment* (Office of the Information & Privacy Commissioner of Ontario, Canada 2011).
[840] These are accountability (Principle 1) and its sub-dimensions (accountability-related questions, policies and procedures, security and risk management; privacy and security training and awareness; audit and compliance); privacy as the default setting (Principle 2); full life-cycle protection (Principle 5); visibility and transparency (Principle 6) and its sub-dimensions (accountability: openness; and compliance); and respect for the user privacy (Principle 7) and its sub-dimensions (questions on policies and procedures, expectations of privacy and consent).
[841] De Hert and Wright (2012).

permissible limitations is an inescapable step in a legal analysis of interference, but it cannot replace a clear understanding of the rights under scrutiny.

While acknowledging the positive features of PIAs, a methodology for assessing interference or compliance with rights requires a different approach. Moreover, this enquiry should factor in work by information security specialists on methodologies to assess threats to network and information systems and privacy (as understood in computer science) to bridge the legal and technological understanding of the same referents, as I try to do in the next section.

3 THE PROPOSED METHODOLOGY

Here I develop a methodology to identify the impact on privacy rights of technologies used to prevent/mitigate, perpetrate and detect/investigate cybercrimes. The methodology is composed of five steps, each illustrated in a different section.

The first step (section 3.1) consists of building a matrix based on mapping the correspondence of cybercrimes as defined in EU applicable law to existing, real world threats and the technologies used to prevent, perpetrate and detect them. In other words, it consists in linking existing literature on threats and technologies to legal definitions of cybercrimes.

The second step (section 3.2) is to appraise the impact of such technologies on information security and privacy (technically understood). It requires establishing the link between the technologies, information security canons and privacy canons, by relying on STRIDE and LINDDUN respectively, as well as on-going work on privacy by design.

The third step (section 3.3) is to assess whether these technologies are susceptible to interfere with privacy rights and their essence or core. It can be dissected into three stages. First, appraising the intrusion into a fundamental right entails answering the question: what does that fundamental right mean? It obliges us to perform the exercise, in the abstract, of dissecting the right into its substantive characteristics or attributes. The idea of attributes of rights is taken from, and builds upon, the work on indicators. Such an exercise, in turn, allows us to perform the second step, which requires identifying the essence or core of the right,

based on the revisited core-periphery theory of fundamental rights of Alexy, the intrusion into which would be prohibited. Finally, it is necessary to link the technologies analysed, their impact on privacy canons, and on the attributes (core) of rights.

The fourth step (section 3.4) consists in appraising the permissibility of such technologies, based on the type of impact and level of intrusion they have on privacy rights, and hence the balancing test enhanced by the core-periphery model.

The final step (section 3.5) will allow comparing technologies on the basis of their impact on privacy rights and cybercrime, to appraise whether strategies to protect the first and prevent the second are complementary, or rather whether there is a tension. The SURVEILLE method will be used here. The technologies can be grouped according to Clarke's revisited taxonomy: interference, compliance and synergy. The SurPRISE method could then be used to choose technologies. A diagram summarizing the steps concludes this chapter (section 4).

3.1 STEP 1: DEVELOPING A MATRIX OF OFFENCES, THREATS AND TOOLS

The first step of the method consists in 'mapping the field' by building a matrix for the legal study of tools used in relation to a given cyber-related offence. Such a matrix, which is visually represented in Table 7 below, can be built in two steps.

The first step consists in analysing the substantive relation between crime and crime-related tools, and can be divided into three further moves: i) the legal definition of a cybercrime in accordance with existing applicable law; ii) the correspondence between the offence and known threats or behaviour; iii) a consideration of the affected layer of the cyber-domain. This last move is relevant because the level of the cyber domain at which the offence takes place determines its wider implications, notably for privacy rights, and the applicable legal framework.[842]

The second step consists in listing the tools used in relation to a given offence to either prevent/mitigate, detect/investigate (forensics), or perpetrate a cybercrime. To this effect, it is

[842] This entails an understanding of cyberlaw that embraces the infrastructure needed to exchange data, and related harms, in addition to information and intermediaries considered in Jacqueline Lipton, *Rethinking Cyberlaw. A new Vision for Internet Law* (Edwar Elgar Publishing 2015).

necessary to perform an analysis of existing literature and annual reports on threat scenarios (such as ENISA's,[843] Microsoft's, OWASP's etc.).

Tech/tool **Crime**	**Substantive issues**			**Tools used to**		
	i) Definition/ legal basis	ii) Corresponding threats/ behaviour	iii) affected block of cyber	Perpetrate	Detect/ Investigate	Prevent/ Mitigate
Illegal access	Dir. 2013/40/EU art. 3	Hacking, cracking, hacktivism				
Illegal interception	Dir. 2013/40/EU art. 6	Snooping, sniffing, spyware				
Data interference	Dir. 2013/40/EU, art. 5; Dir. 2001/29/EC, art 7	Worms, viruses, malware, tampering, defacing				
System interference	Dir. 2013/40/EU, art. 4 and Recital 5 + [a-contrario e-Privacy Dir.]	(Distributed)denial of service, botnets DNS poisoning, spamming				
Tools used to commit crimes	Dir. 2013/40/EU, art. 7; CFD 2001/413/JHA, art. 4; Dir. 2001/29/EC, art. 6 and 7 without criminalization	Production, distribution/making available and sale of tools, programmes, kits				
Computer-related fraud	CFD 2001/413/JHA, art. 3	Illegal data/system interference (for transferring money); cyber-extortion				
Computer-related forgery	CFD 2001/413/JHA, art. 4 + a-contrario eIDAS Reg.	Tampering; Phishing; spear phishing;				
Copyright infringement	Dir. 2001/29/EC, arts. 6 and 7					
Child-pornography online	Dir. 2011/92	Blocking or removing web pages; filtering				
Identity theft	Dir. 2013/40/EU art. 9 (5) (aggravating circumstance) and recital 14					
e-recruitment of terrorists	Proposed counter-terror Dir.					
Large-scale attacks	Dir. 2013/40/EU art. 9 (3) + proposed counter-terror Dir.					
Xenophobic and hate speech	/	e-propaganda				
Cyber-bullying	/	trolling				

Table 7 Draft matrix

[843] See, for instance, Louis Marinos, Adrian Belmonte and Evangelos Rekleitis, *ENISA Threat Landscape 2015* (European Network and Information Security Agency (ENISA), 2016).

3.2 STEP 2: DETERMINING THE IMPACT OF TOOLS AND TECHNOLOGIES ON INFORMATION SECURITY AND PRIVACY CANONS: STRIDE, LINDDUN AND ENISA'S WORK ON PBD TECHNIQUES

The first step built the link between an existing offence (cybercrime), the threat it embodies and the technology relied upon. Step two shows the link between the technology and the threat they represent to both cybersecurity and privacy. In the context of the SURVEILLE projects I proposed looking at the functions performed by a technology to understand its impact on rights.[844] A more suitable understanding of the impact of tools in the context of cybersecurity, seen from a technological perspective, is the established analysis of threat modelling (STRIDE and ENISA), and the experimental yet promising work on privacy canons (LINDDUN and ENISA). This requires moving in the unfamiliar territory of information security and computer science (the necessary disclaimer being that expert validation would be needed to carry this forward). This step includes three moves.

First of all, I identify the dichotomy between threat and protection goals in relation to information security; then I do the same in relation to privacy; finally, I work out the cross-relationships (relationship between threats, tools and canons).

3.2.1 FIRST MOVE: INFORMATION SECURITY THREATS AND PROTECTION GOALS

Technologies embody threats[845] in that they imperil information security canons or protection goals, a concept anticipated in chapters 3 and 4. The basic information security canons are the triad of confidentiality, integrity and availability,[846] to which more have been added over time. Standardization bodies such as the International Organization for

[844] Porcedda (2013), *Paper Establishing Classification of Technologies on the Basis of their Intrusiveness into Fundamental Rights* (SURVEILLE Project Deliverable D2.4).

[845] ENISA defines threats as "Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service." European Network and Information Security Agency (ENISA), 'Glossary' (*ENISA*) <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary> accessed 2 February 2015. Following ISO/IEC PDTR 13335-1, an asset is "Anything that has value to the organization, its business operations and their continuity, including Information resources that support the organization's mission."

[846] George Danezis and others, *Privacy and Data Protection by Design – from Policy to Engineering* (ENISA 2014); Kim Wuyts, *LINDDUN: a privacy threat analysis framework*.

Standardization (hereafter ISO) and the International Telecommunication Union[847] (hereafter ITU) have provided working definitions of the term. Table 8 shows the definitions of the most common security goals provided by ENISA[848] and the ITU:

[847] International Telecommunication Union (2015).
[848] European Network and Information Security Agency (ENISA).

Info security canons	ITU	ENISA
Authorization / Control	**ITU only**: 1. The granting of rights, which includes the granting of access based on access rights. Note – This definition implies the rights to perform some activity (such as to access data); and that they have been granted to some process, entity, or human agent. 2. The granting of permission on the basis of authenticated identification. 3. The act of giving access to a service or device if one has the permission to have the access.	
Authentication	**ITU only***:* 1. The process of corroborating an identity. Note – See principal and verifier and the two distinguished form of authentication (data origin auth. + entity auth.). Authentication can be unilateral or mutual. Unilateral authentication provides assurance of the identity of only one principal. Mutual authentication provides assurance of the identities of both principals. 2. The provision of assurance of the claimed identity of an entity. 3. See data origin authentication, and peer entity authentication. The term "authentication" is not used in connection with data integrity; the term "data integrity" is used instead. 4. The corroboration of the identity of objects relevant to the establishment of an association. For example, these can include the AEs, APs, and the human users of applications. Note – This term has been defined to make it clear that a wider scope of authentication is being addressed than is covered by peer-entity authentication in CCITT Recommendation ITU-T X.800. 5. The process of verifying the claimed identity of an entity to another entity. 6. The process intended to allow the system to check with certainty the identification of a party.	
Availability	The property of being accessible and useable upon demand by an authorized entity.	The fact that data is accessible and services are operational.
Confidentiality /data secrecy	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (Information can be either in transfer or stored)	The protection of communications or stored data against interception and reading by unauthorized persons.(ENISA) The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (ISO/IEC PDTR 13335-1)
Integrity	The property that data has not been altered or destroyed in an unauthorized manner.	The confirmation that data which has been sent, received, or stored are complete and unchanged. (ENISA) The property that data has not been altered or destroyed in an unauthorized manner. (ISO/IEC PDTR 13335-1)
Non-repudiation	*1*. The ability to prevent a sender from denying later that he or she sent a message or performed an action. 2. Protection from denial by one of the entities involved in a communication of having participated in all or part of the communication. 3. A process by which the sender of a message (e.g. a request on a pay-per-view) cannot deny having sent the message.	The property that ensures that the actions of an entity may be traced uniquely to the entity. (ISO/IEC PDTR 13335-1) This may cover non repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. (ENISA)
Utility	**ITU only** The information is relevant and useful for the purpose for which it is needed	

Table 8 Information security canons/protection goals

The identification of threats to canons, called threat modelling, is part of risk[849] assessment,[850] in turn a part of risk management,[851] which belongs to information security management. Maintaining security is seen as an endless process (such as Microsoft's secure development lifecycle[852]),[853] as exemplified by the assumption that "security is like a chain. It is as strong as its weakest link."[854]

In expert circles, threat modelling is performed by analysing a system to be protected through the lenses of a potential attacker. There exist several models of threat modelling,[855] but a reference point in the field is Microsoft's STRIDE model.[856]

The name is the acronym of the threats that a network and information system could suffer from: spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege. These threats are the negation of information security canons described above. Spoofing means that the attacker replaces the verified user of a system. Tampering consists in corrupting the data. Repudiation means that an action cannot be correctly associated with its origin. Information disclosure consists in making confidential information

---

[849] ENISA defines risk as in ISO/IEC PDTR 13335-1: The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization." Vulnerabilities are, following ITSEC, "The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved."

[850] ENISA defines it as "A scientific and technologically based process consisting of three steps, risk identification, risk analysis and risk evaluation."

[851] ENISA defines risk management as "The process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options. The ISO produced a number of standards based on ISO 27005:2011, currently under revision: (http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=64141).

[852] See at Microsoft, 'Security Development Lifecycle' (*Microsoft*) <https://www.microsoft.com/en-us/sdl/> accessed 21 October 2015.

[853] Clarke (2001), 'Introduction to Information Security'; European Network and Information Security Agency (ENISA), *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools* (2006).

[854] For an extended description of risk management in the field of information security, see European Network and Information Security Agency (ENISA) (2006), *Risk Management*, 8. Management systems are based on assumptions, e.g, people are more important than technology for the maintenance of security (information security is endangered more by employees rather than outsiders) and the degree of security depends on three factors: the risk you are willing to take, the functionality of the system and the costs you are prepared to pay.

[855] See at Microsoft, 'SDL Threat Modeling Tool' (*Microsoft*) <https://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx> accessed 21 October 2016; OWASP, 'Threat Risk Modeling (wiki)' (*OWASP*) <https://www.owasp.org/index.php/Threat_Risk_Modeling> accessed 21 October 2016.

[856] Microsoft, 'The STRIDE Threat Model' (*Microsoft*, 2005) <https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx> accessed 21 October 2016. It is used as the basis for tackling different components of network and information security, such as OWASP's web application vulnerabilities. See at OWASP, 'Application Threat Modelling' (*OWASP*) <https://www.owasp.org/index.php/Application_Threat_Modeling> accessed 21 October 2016. See also Mouna Jouinia, Latifa Ben Arfa Rabaia and Anis Ben Aissab, 'Classification of Security Threats in Information Systems, 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014)' [2014] Procedia Computer Science 489 – 496.

available to illegitimate recipients. Denial of service consists in making a service unavailable as otherwise expected. Finally, elevation of privileges consists in gaining access to a system without having the necessary privileges. The table below shows the name of the threat, an example of its implementation, and the corresponding infringed security canon.

Threat	**Example of threats on the Web**[857]	**Security canon/property**
Spoofing	Replacing a malicious web server with a fake web server	Authentication
Tampering	Fiddling with user data travelling on from web server to client	Integrity
Repudiation	Deleting the audit logs	Non-repudiation
Information disclosure	Accessing profile data directly in a database	Confidentiality
Denial of Service	Preventing access to a web server by flooding it with TCP/IP packets	Availability
Elevation of privilege	Impersonating an administrator (after having spoofed the authentication packets in the Lightweight Directory Access protocol)	Authorization

Table 9 Information security canons and corresponding threats in the STRIDE model

Note that the model does not include the information security property 'utility'. The model is composed of nine steps,[858] the fundamental of which is the fifth one, i.e. decomposing the application into data flow diagrams of each component that can be seen as a sub-application. Data flow diagrams are the essential sub-units to which the STRIDE model is applied.

3.2.2 SECOND MOVE: PRIVACY THREATS AND PROTECTION GOALS

It is important to clarify upfront that there can be sharp differences between the notion of privacy used in computer science, and the legal one expounded in chapter 2. Discrepancies

[857] Examples taken from Microsoft, 'Applying STRIDE' (*Microsoft*, 2005) <https://msdn.microsoft.com/en-us/library/ee798544%28v=cs.20%29.aspx> accessed 21 October 2016.

[858] These are: first, defining the functionalities of an application; second, listing the systems on which the application depends, i.e. what the application cannot control; third, understanding the application, being aware of the desired security; fourth, being aware of possible security flaws deriving from the system on which the application depends; fifth, decomposing the application into data flow diagrams of each component that can be seen as a sub-application; sixth, building a taxonomy of threats (e.g. STRIDE); seventh, linking the taxonomy of threats to the application and its sub-elements, for instance by using tree patterns; eighth, determining the likelihood that the threat could materialize, i.e. the risk.

between the technical and legal understandings must be taken into account when dealing with potential overlaps. The ITU defines privacy as "1. The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. 2. A mode of communication in which only the explicitly enabled parties can interpret the communication. This is typically achieved by encryption and shared key(s) for the cipher."[859] Note the conflation between the different understandings of privacy rights. Indeed, in relation to point 1, the ITU warns "since this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security."

Anderson and Clarke[860] point out that confidentiality, secrecy and privacy are often incorrectly conflated. For Anderson, 'secrecy' is a technical term concerning mechanisms to limit the number of entities accessing information;[861] examples are computer access controls and cryptography. Confidentiality concerns the duty to protect an entity's secrets you are aware of. Privacy means the ability to protect your personal information, and also the protection against invasions of one's personal space. Hence, "privacy is secrecy for the benefit of the individual, while confidentiality is secrecy for the benefit of the organization."[862]

Unlike information security, there is little work on threat modelling (including protection goals) in the field of privacy.[863] The LINDDUN project and the ENISA study on engineering PbD[864] fill the gap by defining protection goals, and the former also defines privacy threat modelling. As for protection goals, LINDDUN borrows from Danezis the idea that privacy can be either soft or hard. Hard privacy consists in the minimization of disclosure of information; consequently, the individual does not need to rely on the data controller for protection. It is identified with the protection goal of data minimization: the data, which is not disclosed, is secure. Soft privacy consists in the knowledge that information has been disclosed, and thus the data subject has to trust the data controller(s). Then, taking inspiration from the data protection goals identified by Pfitzman, LINDDUN identifies the relevant privacy canons by dividing them into the two categories of hard and soft privacy canons.

[859] International Telecommunication Union (2015), p. 160, Annex A.
[860] Clarke (2001), 'Introduction to Information Security'.
[861] For a distinction between secrecy in the offline world, and in network and information security, see Peter Swire, 'A Model for When Disclosure Helps Security: What is Different about Computer and Network Security?' (2004) 2 Journal on Telecommunications and High Technology Law.
[862] Anderson (2008), p. 14.
[863] Danezis and others (2014).
[864] Ibid.

Hard privacy canons are: 'unlinkability', 'anonymity and pseudonimity', 'undetectability and unobservability', with the addition of 'plausible deniability' and 'confidentiality'. Soft privacy canons are extracted from applicable law and are 'content awareness' and 'policy and consent compliance'. While acknowledging the importance of availability and integrity to privacy, LINDDUN does not take this into account.

Differently, ENISA's list of protection goals starts from the classic information security CIA triad and then adds unlinkability, transparency and intervenability.

In the absence of a standard (the ISO privacy standard[865] does not address protection goal matters), I attempt to merge the two sets of canons, an attempt which remains experimental until validated. The so merged protection goals produce: unlinkability (including anonymity & pseudonymity, and undetectability & unobservability), plausible deniability, availability, integrity, confidentiality, transparency (including content awareness and policy consent & compliance) and intervenability, as exemplified in Table 10 below:

[865] International Organization for Standarization (ISO), *International Standard ISO/IEC 29100:2011(E) Information technology — Security techniques — Privacy framework* (2011).

Privacy canons	LINDDUN	ENISA
Unlinkability	**Unlinkability**: hiding the link between two or more actions, identities, and pieces of information.	Privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context, and that means that processes have to be operated in such a way that the privacy-relevant data are unlinkable to any other set of privacy relevant data outside of the domain. Mechanisms to achieve or support unlinkability comprise data avoidance, separation of contexts (physical separation, encryption, usage of different identifiers, access control), anonymisation and pseudonymisation, and early erasure or data.
	Anonymity: hiding the link between an identity and an action or a piece of information. **Pseudonymity**: to build a reputation on a pseudonym and the possibility to use multiple pseudonyms for different purposes.	
	Undetectability and unobservability: hiding the user's activities (e.g. impossibility of knowing whether an entry in a database corresponds to a real person)	
Plausible deniability	The ability to deny having performed an action that other parties can neither confirm nor contradict (e.g. a whistleblower can deny his actions) [opposite of non-repudiation]	
Integrity	/	As in information security
Confidentiality	Hiding the data content or controlled release of data content (e.g. encrypted email)	As in information security
Availability	/	As in information security
Transparency	**Content Awareness**: users are aware of their personal data and that only the minimum necessary information should be sought and used for the performance of the function to which it relates.	All privacy-relevant data processing including the legal, technical and organisational setting can be understood and reconstructed at any time. The information has to be available before, during and after the processing takes place. Mechanisms for achieving or supporting transparency comprise logging and reporting.
	Policy and consent compliance: the whole system – including data flows, data stores, and processes – has to inform the data subject about the system's privacy policy, or allow the data subject to specify consent in compliance with legislation, before users access the system	
Intervenability	/	Intervention is possible concerning all ongoing or planned privacy-relevant data processing, in particular by those persons whose data are processed. The objective is the application of corrective measures and counterbalances where necessary. Mechanisms for intervenability comprise established processes for influencing or stopping the data processing fully or partially, manually overturning an automated decision, data portability precautions to prevent lock-in at a data processor, breaking glass policies, single points of contact for individuals' intervention requests, switches for users to change a setting

Table 10 Privacy protection goals for LINDDUN and ENISA

In LINDDUN, each identified privacy canon corresponds to a technology threat from which, similarly to STRIDE, the acronym of LINDDUN is derived: **L**inkability, **I**ndentifiability, **N**on-repudiation, **D**etectability, **D**isclosure of information, content **U**nawareness, policy and consent **N**on-compliance, as exemplified in Table 11 below. Each threat to an item of interest (hereafter IoI, understood variably as a user, action, content etc.) is defined from the perspective of the attacker. Thus, 'linkability' means being able to establish whether two IoIs are related. 'Identifiability' means connecting a user to an IoI. 'Non-repudiation' allows proving that a user has performed a certain action. It should be noted that the authors believe that, unlike for security, this is a threat to privacy. This conclusion would have required an additional degree of detail, based precisely on the distinction between soft and hard privacy elaborated by the authors. In fact, non-repudiation could be deemed to be a threat only in the case of hard privacy, and only when users actively pursue repudiation. In all other cases, non-repudiation is desirable because it is key to the accountability of data controllers. The problem, once more, derives from a conflation between privacy rights and an unrefined understanding of their subtleties. 'Detectability' means that an IoI exists. 'Information disclosure' refers to loss of confidentiality. 'Content unawareness' means that either too much, or the wrong information has been disclosed, leading to the identification of wrong decisions. Finally, 'policy and consent non-compliance' indicates the case in which a system disregards the privacy policy it purports to respect.

Privacy canons as chosen by LINDDUN	Threats to canons
Hard privacy	
Unlinkability	Linkability
Anonymity and Pseudonimity	Identifiability
Plausible deniability	Non-repudiation
Undetectability and unobservability	Detectability
Confidentiality	Disclosure of information
Soft privacy	
Content awareness	Content unawareness
Policy and consent compliance	Policy and consent non-compliance

Table 11 LINDDUN privacy threat modelling

LINDDUN follows the same steps as STRIDE (but does not reach the stage of risk analysis). Therefore, the most fundamental step is the identification of data flow diagrams to

which the threats are applied.[866] Based on such associations, it becomes easier to study mitigation strategies, in the form of privacy enhancing technologies (hereafter PETs) (see infra, section 3.5).

ENISA did not propose a privacy threat model; however, the only canon identified by ENISA that was not considered by LINDDUN is intervenability, the threat to which can be identified, with a good degree of confidence, in non-intervenability, understood as the inability or impossibility to intervene at any level of the system to prevent or mitigate the threat.

3.2.3 Third move: linking information security and privacy protection goals with threats

The STRIDE methodology allows linking the offences listed within the Cybercrime Convention with the features, or functions, of the technologies used to perpetrate, prevent/mitigate, or detect/investigate cybercrimes: the LINDDUN and ENISA methodology enable us to compare the extent to which such threats concern the technological understanding of privacy or not, as done in Table 7, where the star symbol (*) denotes the correspondence between a privacy protection goal and an information security one, notably CIA goals. It should be noted that the privacy threats I propose represent an attempt that remains experimental until validated.

Privacy protection goals	Threats
Unlinkability- Anonymity and Pseudonymity - Undetectability and unobservability	Linkability – Identifiability – Detectability
Plausible deniability	Non-repudiation
Integrity*	Tampering
Confidentiality*	Disclosure of information
Availability*	Denial of Service
Transparency	Content unawareness - Policy and consent non-compliance
Intervenability	Non-intervenability

Table 12 Synthesis of privacy threat modeling

[866] Kim Wyuts, Riccardo Scandariato and Wouter Joosen, *LIND(D)UN Privacy Threat Tree Catalog* (Report CW 675, KU Leuven, 2014).

The following information security canons and threats taken from STRIDE have no immediate correspondence with privacy canons: authentication/spoofing; non-repudiation/repudiation; authorization/evaluation of privilege. Of these, non-repudiation is the only one that can have an ambiguous impact on privacy, taking into account the caveats identified above. It can be anticipated here that non-repudiation is likely to be problematic for the confidentiality of communications, but necessary for the protection of personal data. Furthermore, no mention is made of the property 'utility'. I will elaborate this further in chapter 8.

3.3 STEP 3: THE USE OF ATTRIBUTES AS A BRIDGE BETWEEN PRIVACY CANONS AND AN ANALYTICAL TEST OF PERMISSIBLE LIMITATIONS

Step 3 assesses whether the technologies identified in step 1 and analysed through step 2 are susceptible to interfere with privacy rights and their essence or core. This step would technically be part of a test for permissible limitations, however in practice it consists of laying bare what should be 'known' before, or in order to start, a test for permissible limitations: the attributes of rights, their core, and their interaction with protection goals. Each point corresponds to a move within this step.

Such moves aim at redressing some of the pitfalls of the test for permissible limitations (balancing) discussed in section 2 above, and stems directly from the attempt to correct the test for permissible limitations by adding the analysis of interference with the 'core' or 'essence'. In fact, talking about cores or essences begs the question as to what constitutes the peripheries of a right. The answer proposed here consists in using the concept of 'attributes' as the intrinsic and distinctive substantive dimensions of a right, developed in the context of work on indicators performed by the OHCHR[867] (supported by the Fundamental Rights Agency[868]), and the UK Equality and Human Rights Commission.[869]

[867] United Nations (2006), p. 3.
[868] Fundamental Rights Agency, *Using indicators to measure fundamental rights in the EU: challenges and solutions* (2nd Annual FRA Symposium Report, 2001).
[869] Jean Candler and others, *Human Rights Measurement Framework: Prototype panels, indicator set and evidence base* (Equality and Human Rights Commission 2011).

Attributes are "a limited number of characteristics of [a given] right." (…). To the extent feasible, the attributes should be based on an exhaustive reading of the standard, starting with the provisions in the core international human rights treaties; (…) the attributes of the human right should collectively reflect the essence of its normative content (...) To the extent feasible, the attributes' scope should not overlap."[870] They represent the synthesis of what would otherwise be the 'narrative' on legal standards of a human right. In the context of the OHCHR work, attributes are the first step to build structural indicators, one of three[871] sub-indicators which measure the commitment of a state towards certain human rights objectives.[872]

In the context of this enquiry, attributes can be used as a powerful instrument to capture the granularity of the intrusiveness of surveillance technologies into fundamental rights. In fact, they can help identify cores of rights, the intrusion into which would be impermissible. In this sense, the identification of attributes is a preliminary step for the identification of core(s), and therefore comes logically before them. Some attributes may thus be seen as peripheral, while other attributes will coincide or express a core area.

An attempt to perform such an exercise, taking into account the intrinsic characteristics and interrelatedness, interdependence and indivisibility of human rights,[873] was performed in my previous work within the SURVEILLE project.[874] Here I intend to develop such an approach. The attributes for the right to private and family life (privacy), the focus of chapter 6, are derived from the Human Rights Measurement Framework developed by the UK Equality and Human Rights Commission.[875] The instructions provided by the OHCHR[876] will be followed to study the right to the protection of personal data, which has not undergone yet the thorough process of identification of attributes illustrated in Figure 4.

[870] United Nations (2012), p. 31.
[871] The other two sub-indicators correspond to the criteria of process and outcome.
[872] Structural indicators include the number of international human rights treaties signed and ratified, or the adoption of specific laws or mechanisms for the implementation of human rights. The focus is on domestic laws, policy and strategies in relation to a specific right. It should be noted that good indicators are contextually relevant for the jurisdictions under analysis.
[873] Limitations to fundamental rights do not affect such qualities.
[874] Porcedda (2013), *Paper Establishing Classification of Technologies on the Basis of their Intrusiveness into Fundamental Rights* (SURVEILLE Project Deliverable D2.4).
[875] Candler and others (2011). The HRMF provides continuous and updated evidence of incorporation of human rights standards into public policy and of the existence of a culture of human rights. To this end, it maps violations as well as proactive public policy approaches.
[876] United Nations (2006), p. 3.

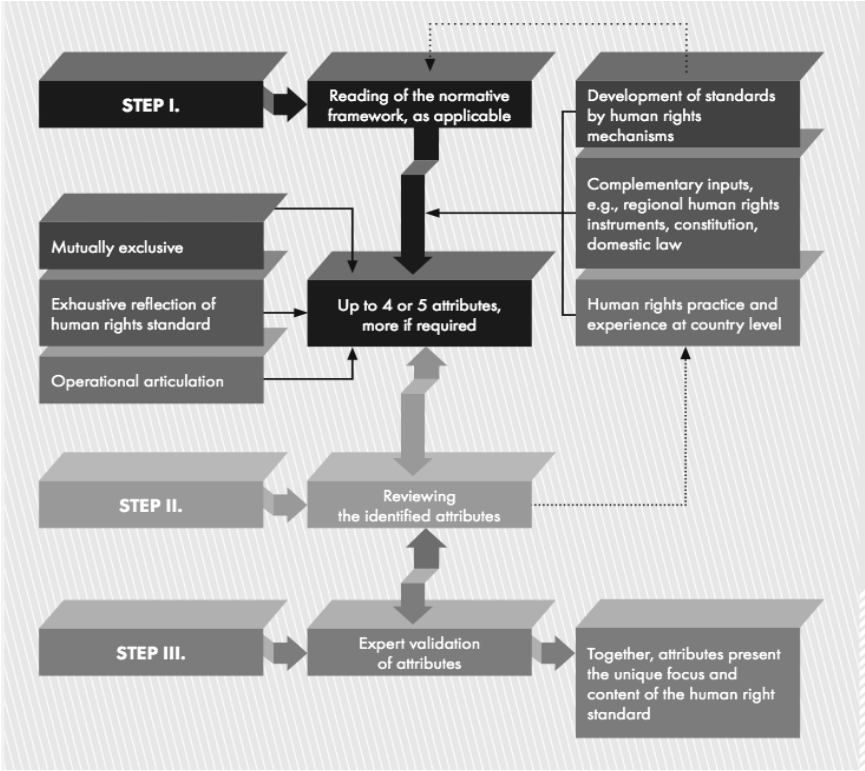


Figure 4 Procedure to extract the attributes, OHCHR, p. 72

First, it is necessary to discern the applicable legal framework, which includes international as well as regional instruments, case law and authoritative interpretations. In this thesis, the selection of attributes will be based on the Charter, since it encompasses the progress made by previous human rights instruments. Second, the attributes identified should be as few as possible, mutually exclusive and able to capture the full meaning of the right. The second and third steps consist in reviewing the attributes, and validating them respectively.

In sum, appraising the intrusion into a fundamental right entails answering the question: what does that fundamental right mean? It obliges us to perform the exercise, in the abstract, of dissecting the right into its substantive characteristics or attributes. Such an exercise, in turn, allows performing the second step, which requires identifying the essence or core of the right, the intrusion into which would be prohibited. This is the objective of chapters 6 and 7.

The identification of attributes and cores enables us to link the legal understanding of the rights with the technical understanding of privacy and information protection goals and of threat scenarios discussed in step 2. This step will be performed in chapter 8.

3.4 STEP 4: THE TEST FOR PERMISSIBLE LIMITATIONS TO FUNDAMENTAL RIGHTS

The identification of attributes is a preliminary step for the definition of core(s) and hence of the determination as to whether a technology is permissible or impermissible. The contextual assessment will derive from the application of an analytically rigorous test for the permissibility of restrictions of fundamental rights, which belongs to the fourth step of the methodology. An analytically rigorous test for the permissibility of restrictions of fundamental rights, as for instance elaborated by the former United Nations Special Rapporteur on respecting human rights while countering terrorism, based on the ICCPR, is the following:

> *"(a) Any restrictions must be provided by the law (paras. 11–12);*
> *(b) The essence of a human right is not subject to restrictions (para. 13);*
> *(c) Restrictions must be necessary in a democratic society (para. 11);*
> *(d) Any discretion exercised when implementing the restrictions must not be unfettered (para. 13);*
> *(e) For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim (para. 14);*
> *(f) Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instruments amongst those, which might achieve the desired result; and they must be proportionate to the interest to be protected (paras. 14–15);*
> *(g) Any restrictions must be consistent with the other rights guaranteed in the ICCPR (para. 18)."*[877]

It should be recalled that any use of a technology that impaired the essence, or core, of a fundamental right, even if authorized to do so by a legal basis, would be impermissible, and therefore unlawful. The parts of the legal basis authorizing the use of a technology in a way that infringed any core of the fundamental rights would also be impermissible. Chapters 6 and 7 will address the test for permissible limitations in Union law.

[877] Scheinin (2009), *Report on Human Rights and Fundamental Freedoms while Countering Terrorism*, paragraph 17 (footnotes omitted, emphasis added). The bracketed references to numbered paragraphs relate to General Comment No. 27 by the Human Rights Committee, Human Rights Committee (1999), *General Comment n. 27*. The same elements for a permissible limitations test were presented in Scheinin and Vermeulen (2011), 41. See also Porcedda, Vermeulen and Scheinin (2013).

3.5 STEP 5: APPRAISING THE COMPLEMENTARITY OF CYBERCRIME PREVENTION AND THE PROTECTION OF PRIVACY RIGHTS

The final step will allow comparing technologies on the basis of their impact on privacy and cybercrime, to appraise whether strategies to protect the first and prevent the second are complementary, or rather whether there is a tension. This includes three moves.

The first move of step 5 is the implementation of the rigorous test of scoring built within the SURVEILLE project, which can be applied to rights dissected in their attributes.

Second, and in essence, this enquiry tries to investigate whether cyber-security and privacy rights can be complementary. How to qualify complementarity in legal terms? A possibility is to refer to a well-established typology, the tripartite duty to "respect, protect and fulfil", which customarily identifies state obligations towards human rights.[878] The

> *"obligation to respect (...) requires States parties to refrain from interfering directly or indirectly with the enjoyment of a right. The obligation to protect requires States parties to take measures that prevent third parties from interfering with the enjoyment of the right (...). The obligation to fulfil includes the obligations to provide, facilitate and promote that right. It implies that States parties should adopt appropriate legislative, administrative, budgetary, judicial and other measures to ensure its full realization".*[879]

'Respect, protect and fulfil' could be abstracted from their reference to state obligations and used to the effect of describing the results of the impact of a technology on a certain right. Technologies that 'respect' are those that refrain from interfering directly or indirectly with the enjoyment of a right. Technologies that protect are those that prevent parties from interfering with the right. Technologies that fulfil are those that provide, facilitate and promote that right.

[878] The typology was promoted in the 1980s by Asbørn Eide, the then Special Rapporteur on the Right to Adequate Food, and successively adopted and further refined by the Committee on Economic, Social and Cultural Rights. Martin Scheinin, 'Characteristics of Human Rights Norms' in Catarina Krause and Martin Scheinin (eds), *International Protection of Human Rights: a Textbook* (Abo Akademi Institute for Human Rights 2009).

[879] The quote is taken from the Committee on Economic, Social and Cultural Rights, General Comment n. 18 (2005), UN doc. HRI/GEN/1/Rev.9 (vol. I) pp. 139-152, at § 22, cited in ibid, p. 27, note 22. See also at: <http://www.fao.org/docrep/w9990e/w9990e03.htm>.

Clarke's classification of technologies[880] bears an interesting analogy to existing human rights jargon. He identified two macro categories of technologies, privacy-invasive technologies (hereafter PITs) and PITs countermeasures (or counter-PITs).[881] PITs are technologies that purposefully invade privacy, or do so as a side effect (depending on how they are used).[882] Counter-PITs are explicitly designed to neutralize the effects of PITs; their power, however, depends on the final implementation. Counter-PITs can be divided into savage and gentle Privacy-enhancing technologies (hereafter PETs).[883] Savage PETs are technologies that enable genuine anonymity, thus pre-empting the effect of PITs. However, they are considered savage because they reduce accountability and foster socially uncooperative behaviour. Gentle PETs are privacy-sympathetic technology, that is, technologies that introduce the middle ground between privacy and accountability, and create pseudonymity. However, their success depends on the trustworthiness of a number of parties. These are intended to balance the interests of privacy and accountability, and are oriented towards protecting pseudonymity rather than anonymity,[884] or the protection of personal data in settings where identity is clear.[885]

Let us look into PITs. PITs are invasive, i.e. intrusive. In legal terms 'intrusiveness' means 'interference', which can be either permissible or impermissible. On the one hand, if the interference is permissible and circumscribed, it qualifies as a 'limitation' of a right. On the other hand, if the interference is impermissible or unrestricted, it qualifies as a 'violation'. The first case corresponds to qualified rights, as is the case of respect for private and family life and protection of personal data. In other words, a technology could be permissible if it interferes with those rights, provided it conforms to the provisions of a rigorous test for permissible limitations discussed above. The second case corresponds to both absolute rights and the 'essence' or 'core' (*supra* section 3.3) of the right to private and family life and protection of personal data, which cannot be interfered with under any conditions. Legal instruments providing for the intrusion into these rights or core areas of rights would be

[880] Roger Clarke, 'Introducing PITs and PETs: Technologies Affecting Privacy' Privacy Law & Policy Reporter <http://www.rogerclarke.com/DV/PITsPETs.html>.
[881] Ibid.
[882] Examples include data-trail generation through the denial of anonymity, data-trail intensification (e.g. identified phones, SVCs, and ITS), data warehousing and data mining, stored biometrics, and imposed biometrics.
[883] On privacy enhancing technologies, see also European Commission, *Promoting Data Protection by Privacy Enhancing Technologies (PETs)* ((Communication) COM (2007) 228 final, 2007); Unabhaengiges Landeszentrum fuer Datenschutz (ULD) (2013).
[884] Clarke, 'Introducing PITs and PETs: Technologies Affecting Privacy'.
[885] Roger Clarke, 'The Legal Context of Privacy-Enhancing and Privacy-Sympathetic Technologies' accessed 5 April 1999.

contrary to fundamental rights, and thus illegal. Therefore, it is possible to distinguish between permissible and impermissible (uses of) PITs. Permissible PITs interfere with the two rights. Impermissible PITs violate rights.

Let us now focus on counter-PITs, which provide different degrees of proactive fulfilment (gentle or savage PETs). Gentle PETs might be said to protect the rights to respect for private and family life and the protection of personal data, or to be weakly complementary to them. Savage PETs may instead fulfil such rights.

"Respect" could be the result of a technology that does not impinge on the two rights, but that does not promote them either; such technologies, building on Clarke's model, could be called 'privacy-compliant technologies'. In this sense, permissible PITs could also be said to 'respect' the two qualified rights.

Therefore, based on the above-mentioned analogy, I suggest to use the following categories of the impact of technologies on rights: i) respect, which is the result of privacy-compliant technologies (but also privacy by design) and permissible PITs; ii) protection, which is the result of gentle PETs, that enable weak complementarity; iii) fulfilment, which is the result of savage PETs, that enable strong complementarity of technology with rights; and iv) violation, which is the result of impermissible PITs.

As a third and final move, at a higher level of abstraction, a possible policy approach to choose between equally legally viable technologies would be the one established within SurPRISE and described *supra* (section 2.1.3).

4 CONCLUDING REMARKS

This chapter addressed hypothesis IV, whereby the combination of the 'principle' of technology neutrality followed by the law and accepted by courts, and the open-ended understanding of rights, leads to the insufficiency of classic legal analysis for appraising the link between cybersecurity and privacy rights.

Starting from a discussion of the merits and limits of existing attempts to appraise the impact of technologies on rights, I have proposed a methodology that could help answer the question as to whether there can be complementarity between a certain understanding of cybersecurity and privacy rights. The steps of the methodology are summarized in the diagram below.

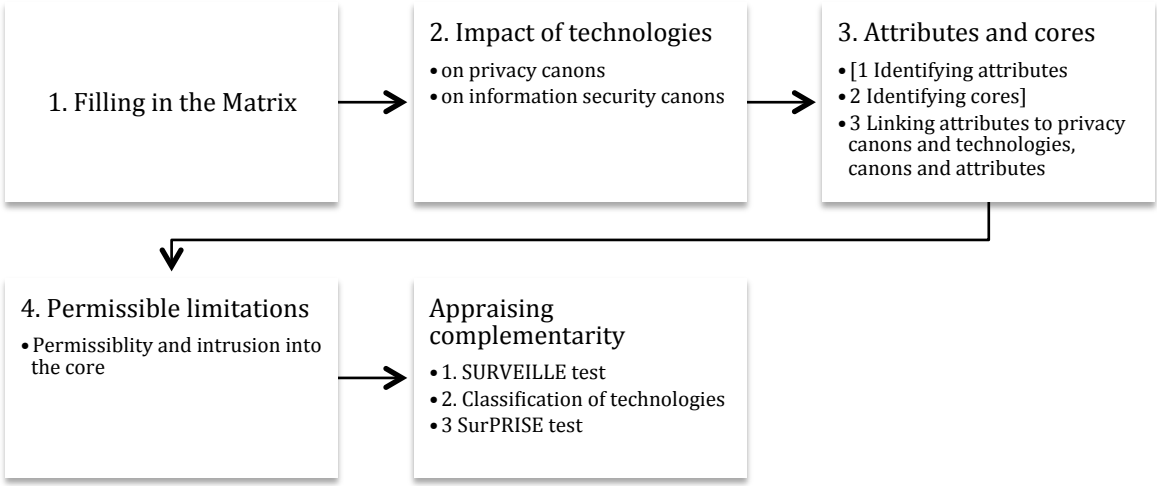


Figure 5 Diagram showing the 5 steps of the methodology

This chapter has offered an (illustrative) overview of steps 1 and 2. Step 3 (moves one and two) is the object of the next two chapters. Chapter 8, the last in this second part of the thesis, will offer a working example of the method.

CHAPTER 6 – THE ATTRIBUTES OF THE RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE

This chapter is dedicated to the identification of the attributes and core(s) of the right to respect for private and family life, based on the procedure for extracting the attributes outlined in chapter 5. The attributes will, in turn, be the basis for the analysis of the relationship between the two rights and cyber security (chapter eight).

Section two starts with an analysis of the sources of the right to respect for private and family life, and its formulation, instrumental in identifying the attributes.

Section three contains the selection of attributes, which builds on existing work by the UK Equality and Human Rights Commission. Attributes are expounded through case law and authoritative interpretations.

In section four I discuss the regime of permissible limitations of article 7 of the Charter, (as a preliminary step for the application of step four of the methodology identified in chapter 5).

Before moving on to the sources of the right, I discuss the procedure for identifying the attributes in the context of EU law.

1 THE PROCEDURE FOR IDENTIFYING THE ATTRIBUTES *VIS-À-VIS* EU LAW

In order to identify the attributes, which should be as few as possible, mutually exclusive, and capable of capturing the full meaning of the right, it is necessary to discern the applicable legal framework, which should include international as well as regional instruments, case law and authoritative interpretations. As noted in chapter 5, reviewing and validating the attributes can only be performed indirectly for this study, based on reference to prominent authors in the field.

The legal framework of reference is EU law. First, this thesis concerns regulatory matters relating to technologies used to perpetrate, prevent or investigate cybercrimes, which constitute implementation of Union law. Second, splitting privacy into two rights is a regional choice made in the Union that is not necessarily reflected in other jurisdictions (though see chapter 7). This also means that the attributes I identify in this chapter are specific to the Union legal framework and, as such, I have no pretence of universal application.

Institutions, bodies, offices and agencies of the Union and Member States[886] are bound by the Charter of Fundamental Rights of the European Union[887] (hereafter the Charter) whenever "implementing" EU law. This means, broadly, "acting within the scope of EU law".[888] In *Åkerberg Fransson* the ECJ clarified that, in situations "where action of the Member States is not entirely determined by Union law…national courts are free to apply national standards of protection of fundamental rights", so long as such standards do not compromise the level of protection afforded by the Charter, as well as the primacy, unity and effectiveness of EU law.[889] In any case, the Court further stated that applicability of EU law entails automatic application of the Charter.[890] Hence, the Charter constitutes the primary document of reference, supplemented by the ECHR[891] (which is the usual instrument of reference for privacy scholars, due to its chronological primacy and the copious case law of the ECtHR on article 8) in the form and to the extent indicated within the Charter, as discussed in the remainder (see also chapter 1).

Additional sources necessary to derive attributes are identified by complementing the sources of rights explicitly listed in the Explanations[892] to the Charter with interdependent instruments, older laws, and sources – whose importance is widely acknowledged in the field – having varying legal force in the EU. Since the right to the protection of personal data is complementary to the right to respect for private and family life, the sources of the former

[886] "The Charter will be applicable when the Member States act as agents for the EU in the context of shared administration, and when they seek to take advantage of a defence to what would otherwise be the applicable EU norm. The Charter should apply to Member States when their action falls within the bounds of a Treaty article, regulation, or decision…the Charter should also be applicable when a Member State implements a directive." Craig (2013), 214.
[887] Charter.
[888] Craig (2013).
[889] Judgment of 17 December 2015 in Åkerberg Fransson, C-617/10, EU:C:2013:105, para 29.
[890] Ibid, para 21.
[891] Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocols No 11 and 14), Council of Europe, ETS n° 005, 4 November 1950.
[892] Charter. Pursuant to articles 52.7 of the Charter and 6.1 TEU, the Explanations have interpretive value. The ECJ stressed that the Explanations have to be taken into account, alongside other provisions of the Treaty and the Charter, to interpret article 51 of the Charter: *C-617/10 - Åkerberg Fransson*, para 20.

flow from the sources of the latter. Their interrelatedness, highlighted in the figure below, must be kept in mind when each source is analysed in relation to a specific right.

The figure below shows the interrelated sources of privacy rights. Therein, the white sections contain the sources relevant for the right to respect for private and family life, whereas the grey sections contain sources unique to the right to the protection of personal data, discussed separately in chapter 7.

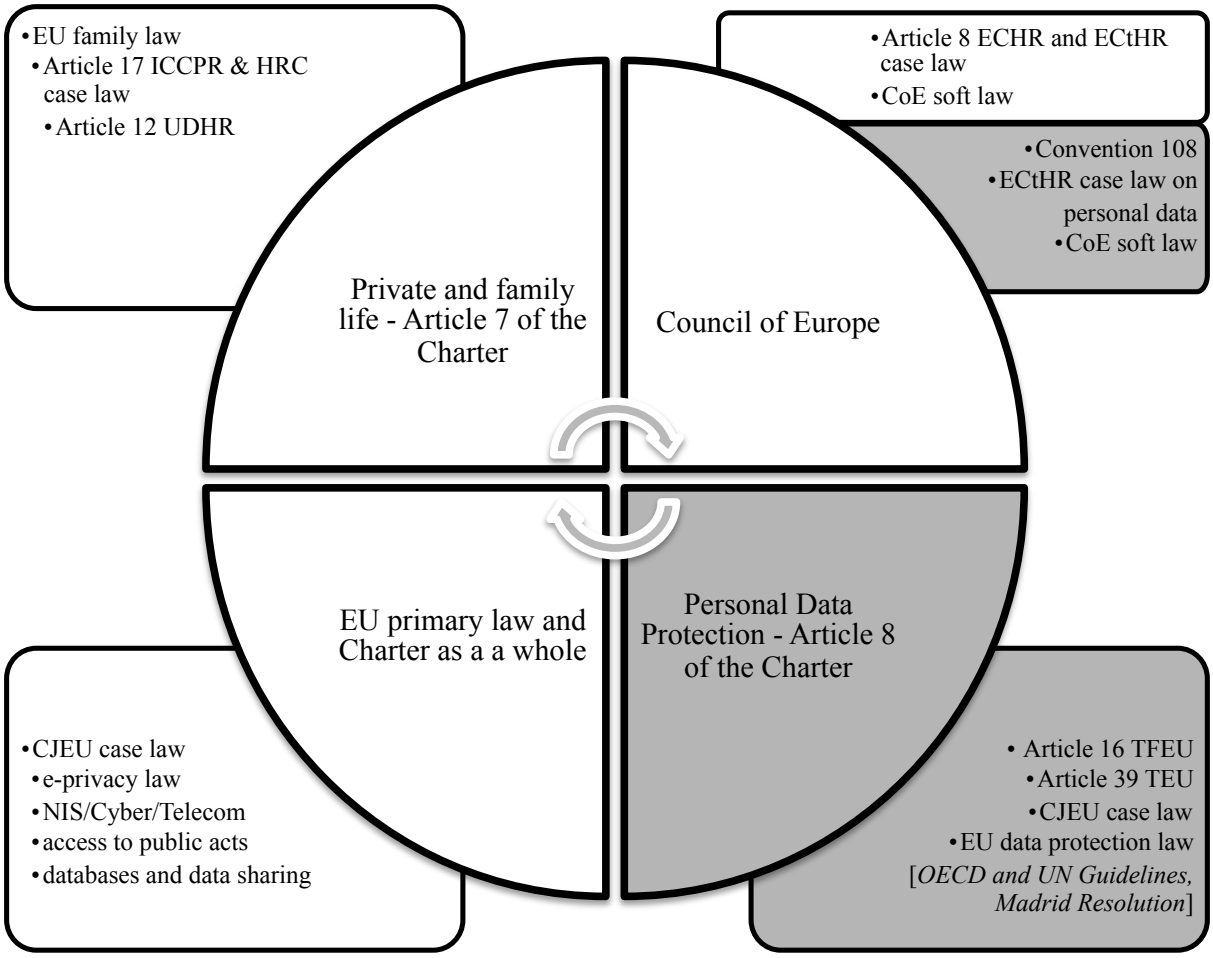


Figure 6 The interrelated sources of privacy rights

The sources of the right to respect for private and family life can be distinguished between instruments binding on the Member States as subjects of international law, such as the ICCPR and the ECHR, and instruments of EU law, binding on the institutions and on the Member States *qua* associates of the Union, such as the Charter, the Treaty, and related secondary law. In this chapter, and more generally in this thesis, I look at the obligations arising from these instruments upon Member States and institutions of the European Union

qua components of the Union. The consequences produced by the interaction of rules of national law that fall outside the remit of EU law, and provisions of international instruments, are beyond the scope of this research. Suffice to recall that, in *Åkerberg Fransson* the ECJ clarified that, although the fundamental rights recognized by the ECHR constitute general principles of Union law, the ECHR "does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into European Union law. Consequently, Union law does not govern the relations between the ECHR and the legal systems of the Member States, nor does it determine the conclusions to be drawn by a national court in the event of conflict between the rights guaranteed by that convention and a rule of national law".[893] The same should apply, *a fortiori*, to the ICCPR.

Hence, the sources of the right to respect for private and family life could thus be summarized as an *ensemble* of (in order of increasing importance): international instruments of soft law adopted by consensus; international law instruments which supply guidelines for the interpretation of rights recognized within EU law (article 12 UDHR and case law on article 17 ICCPR); the case law of the ECtHR, which must be followed insofar as article 7 of the Charter corresponds to article 8 ECHR; and CJEU case law on primary and secondary law. Finally, instruments of EU secondary law represent an implementation of the right which determines its current understanding, but which can be overridden at any time by the Courts.

Each of these sources is discussed and detailed in section two on the attributes, onto which I move now. In particular, the content of the attributes is derived from a different reliance on the sources: a thorough analysis of the judgments of the CJEU (ECJ and General Court) on article 7 *after the Charter acquired primacy* with the entry into force of the Lisbon Treaty (i.e., since December 1st, 2009), hence, from the time when the Court had to interpret cases on the right to private and family life as 'article 7' cases, alongside article 8 ECHR; consultation of ECtHR judgments on article 8 ECHR; and case law of the Human Rights Committee on article 17 ICCPR (hereafter HRC) discussed in the literature.

[893] *C-617/10 - Åkerberg Fransson*, para 44.

2 SOURCES, FORMULATION AND SCOPE OF ARTICLE 7 OF THE CHARTER[894]

This section contains an appraisal of the **sources, formulation, and scope** of article 7 of the Charter. Section 2.1 addresses the **sources** of article 7 of the Charter and the obligations derived therein. I begin by clarifying the relationship between article 7 of the Charter and article 8 ECHR, and I then appraise the input provided by article 12 UDHR and 17 ICCPR. At the same time, I also address matters of obligations stemming from these sources. In section 2.2, I describe the content and scope of article 7, also in the light of the interpretation of articles 12 UDHR and 17 ICCPR.

2.1 SOURCES OF ARTICLE 7 OF THE CHARTER

I begin with an analysis of the primary source of article 7 of the Charter, namely article 8 ECHR (subsection 2.1.1). There, I highlight the extent to which the two provisions correspond and depart from each other. I subsequently analyse secondary sources, articles 12 UDHR and 17 ICCPR, and give account of their close links to article 8 ECHR (subsection 2.1.2). The goal of the analysis is not only to expound the two sets of sources, but also to show their interrelated nature and cross-impact on article 7 of the Charter, whose relevance becomes clear when revising the formulation of the right.

2.1.1 PRIMARY SOURCE: ARTICLE 8 ECHR, AND ITS CORRESPONDENCE TO ARTICLE 7

Pursuant to article 52(3) of the Charter, the articles therein that derive from the ECHR should be interpreted in the light of the case law of the ECtHR, including permissible limitations. The Explanations explicitly identify Article 7 as a right derived from article 8

[894] In this section, subsections 2.1.2 and 2.2 represent a fully revised version of previous work of mine in Porcedda, Vermeulen and Scheinin (2013).

ECHR,[895] which should be read accordingly. Scholarship[896] has been critical of the correspondence between article 7 of the Charter and article 8 ECHR, particularly with respect to permissible limitations. An analysis of existing case law of the ECJ does not allow drawing firm conclusions on the point, even in cases pertaining to a single limb of the right, such as family-related cases. In *Chakroun*, the ECJ mentions both article 8 ECHR and article 7 of the Charter as sources of the right to private life.[897] In other cases, like *McB*, the ECJ stated:

> *"…It follows from Article 52(3) of the Charter that, in so far as the Charter contains rights which correspond to rights guaranteed by the ECHR, their meaning and scope are to be the same as those laid down by the ECHR. However, that provision does not preclude the grant of wider protection by European Union law. Under Article 7 of the Charter, '[e]very one has the right to respect for his or her private and family life, home and communications'. The wording of Article 8(1) of the ECHR is identical to that of the said Article 7, except that it uses the expression 'correspondence' instead of 'communications'. That being so, it is clear that Article 7 contains rights corresponding to those guaranteed by Article 8(1) of the ECHR. Article 7 of the Charter must therefore be given the same meaning and the same scope as Article 8(1) of the ECHR, as interpreted by the case-law of the European Court of Human Rights".*[898]

Differently, in *Dereci*, the Grand Chamber quoted McB in a way that alters the original meaning

> *"… In so far as Article 7 of the Charter of Fundamental Rights of the European Union ('the Charter'), concerning respect for private and family life, contains rights which correspond to rights guaranteed by Article 8(1) of the ECHR, the meaning and scope of Article 7 of the Charter are to be the same as those laid down by Article 8(1) of the ECHR, as interpreted by the case-law of the European Court of Human Rights."*[899]

The Court subsequently gave a valuable indication of the relationship between the two rights:

---

[895] Verbatim "The rights guaranteed in Article 7 correspond to those guaranteed by Article 8 of the ECHR. To take account of developments in technology the word 'correspondence' has been replaced by 'communications'. In accordance with Article 52(3), the meaning and scope of this right are the same as those of the corresponding article of the ECHR. Consequently, the limitations which may legitimately be imposed on this right are the same as those allowed by Article 8 of the ECHR: '1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder". .

[896] González Fuster and others (2013); González Fuster (2014).

[897] Judgment of 4 March 2010 in Chakroun, C-578/08, EU:C:2010:117, para 44.

[898] Emphasis mine. Judgment of 5 October 2010 in McB, C-400/10 PPU, EU:C:2010:582, para 53.

[899] Emphasis mine. *C-256/11 - Dereci and others*, para 70.

> *"Thus, in the present case, if the referring court considers…that the situation of the applicants in the main proceedings is covered by European Union law, it must examine whether the refusal of their right of residence undermines the right to respect for private and family life provided for in Article 7 of the Charter. On the other hand, if it takes the view that that situation is not covered by European Union law, it must undertake that examination in the light of Article 8(1) of the ECHR."*[900]

It is possible to envisage two situations of mismatch between article 7 of the Charter and article 8 ECHR that are relevant for this analysis.

First, as suggested in *Dereci*, the two articles could embody different rights. While the ECJ will hold the final word on the subject-matter, I am arguing that the first of such mismatches concerns personal data protection, which is protected by an autonomous right of the Charter; as far as other rights are concerned, I will come back to this in section 3.

Second, following the Charter and the ECJ, the EU can depart from the interpretation of the ECtHR with a view to grant higher protection, i.e. acknowledging a broader reach, or interpreting permissible limitations differently (which I tackle *infra*, section 4).

2.1.2 ARTICLES 12 UDHR AND 17 ICCPR

As discussed in chapter 2 (section 3.1), there exist two international instruments capable of supplying guidelines for the interpretation of article 7 of the Charter, both of which have strong links with article 8 ECHR. The first international source is article 12 UDHR, which is the root of article 8 ECHR.[901] The first version of article 8 ECHR[902] voted by the Committee on Legal and Administrative Questions included the reference "as laid down in article 12 of the Declaration on Human Rights of the United Nations".[903] According to Rehof, the relationship between the two provisions is bidirectional, in that the copious case law relating to article 8 ECHR represents a legally binding elaboration of the principles enshrined in article 12 for those who are party to the Convention.[904] Article 12 UDHR, moreover, laid the

[900] Emphasis mine. Ibid, para 72.
[901] Connections go beyond article 8. As mentioned in the preamble, the Convention was in fact a first step "for the collective enforcement of certain of the rights stated in the Universal Declaration of Human Rights". The travaux préparatoires testify to such connection. Council of Europe.
[902] Proposed by M. Rolin (Belgium) and M. Teitgen (France). Ibid.
[903] Ibid.
[904] Lars Adam Rehof, 'Universal Declaration of Human Rights – Common Standard of Achievement' in Asbjorn Eide and Gudmundur Alfredsson (eds), (Scandinavian University Press 1995).

basis for the second relevant international instrument, article 17 ICCPR,[905] which is to date the geographically most widely endorsed provision on 'privacy'.[906] The Committee of Experts on Human Rights had explicitly said that "due attention should be paid to the progress which had been achieved in this matter by the competent organs of the United Nations".[907] Article 17 ICCPR, however, was only introduced in 1953 under the impulse of the Philippines' delegation,[908] so there is no direct cross reference between article 8 ECHR and article 17 ICCPR. Article 17, however, is enshrined in an instrument that is legally binding for the Member States.

In the following section, article 7 Charter/8 ECHR are compared or contrasted with article 12 UDHR/17 ICCPR.

2.2 FORMULATION AND SCOPE OF ARTICLE 7 OF THE CHARTER

As for the formulation of the right, article 7 of the Charter reads, "Everyone has the right to respect for his or her private and family life, home and communications." In what follows, I expound the legal meaning of the right through its formulation.

2.2.1 "EVERYONE HAS THE RIGHT TO"

Article 7 of the Charter is identical to the positive formulation (i.e. having a right to) of article 8 ECHR. Conversely, article 12 UDHR and article 17 ICCPR begin with a 'negative' formulation[909] "*1. No one shall be subjected to arbitrary (or unlawful[910]) interference with his privacy, family, home or correspondence, nor to (unlawful) attacks to their honour or reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.*"

[905] The *travaux préparatoires* of article 17 of the International Covenant on Civil and Political rights also highlight a direct line with article 12 UDHR, whereas there is no direct connection with article 8 ECHR, but in any case they are linked (see note *supra*).
[906] Scheinin (2009), *Report on Human Rights and Fundamental Freedoms while Countering Terrorism*. 167 states are parties to the Convention, available at: http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en.
[907] Council of Europe (1956), p. 4.
[908] Ibid.
[909] Scheinin (2009), *Report on Human Rights and Fundamental Freedoms while Countering Terrorism*.
[910] The adjective 'unlawful' was not part of the original formulation of article 12 UDHR, and has been added in article 17 ICCPR.

Article 12's negative formulation (forbidding interferences with), which is reinforced by the second paragraph, is borrowed from the 4th Amendment to the US Constitution "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated", a formulation that was preferred by the chairman.[911] According to Morsink, this formulation is peculiar not only because other articles enshrined in the Declaration are construed positively, but also because most of the constitutions of the countries protecting the right[912] construed it in terms of inviolability (with reference to home and communications). This was especially the case of Latin American states' constitutions, which were particularly active in proposing the insertion of the article.[913] While both article 17 ICCPR and 8 ECHR are explicitly modelled on article 12 UDHR, the *travaux préparatories* of the latter leave unexplained the reason why a positive formulation was preferred.

2.2.2 "RESPECT FOR": VERTICAL AND HORIZONTAL OBLIGATIONS

Similarly to article 8 ECHR, Article 7 of the Charter features the word "respect". The *travaux préparatories* do not clarify the reasoning behind such choice, which has paved the way to a lively debate, although the ECtHR has focussed on the notion of 'interference' in the second paragraph, thus interpreting the article *a contrario*.[914] The discussion is important, as it introduces the issue of obligations (and scope).

While a *prima facie* interpretation of the wording seems to suggest that the right only embodies a negative obligation to "refrain from" infringing (inaction), the meaning is more nuanced. The ECtHR, in fact, has clarified that article 8 ECHR entails positive obligations

[911] Morsink (1999).
[912] A list of the national constitutions/fundamental laws containing a right to privacy was provided in the International Bill of Rights Documented Outline. They are: Afghanistan, Argentina, Belgium, Bolivia, Brazil, Belorussia, Chile, China, Costa Rica, Cuba, Czechoslovakia, Denmark, Dominican Republic, Ecuador, Egypt, El Salvador, Ethiopia, Greece, Guatemala, Haiti, Honduras, Iceland, Iran, Lebanon, Liberia, Luxembourg, Mexico, Netherlands, Nicaragua, Norway, Republic of Panama, Paraguay, Peru, Philippines, Poland, Sweden, Syria, Turkey, Uruguay, Ukraine, Union of Soviet Socialist Republics, United States (4th amendment) and Yugoslavia. Note that many of the common law countries do not have a written constitution. Some of these constitutions predate the article written by Warren and Brandeis (United Nations, Economic and Social Council, *Commission on Human Rights Drafting Committe. International Bill of Rights* (E/CN4/AC1/3/ADD1 Part 1, 1947). Morsink (1999).
[913] Morsink (1999).
[914] Vincenzo Zeno-Zencovich, 'Articolo 8. Diritto al Rispetto della Vita Privata e Familiare' in Benedetto Conforti e Guido Raimondi Sergio Bartole (ed), *Commentario alla Convenzione Europea per la Tutela dei Diritti dell'Uomo e delle Libertà Fondamentali* (Cedam 2001).

(actions)[915] for the state: "in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective 'respect' [for family life]".[916] The term 'respect' might simply remind the competent authorities that private and family life are a *fait accompli*, a situation that predates the state (and possibly any political organization), which must be protected. To this effect, in Marckx v. Belgium, the ECtHR stated, "by guaranteeing the right to respect for family life, Article 8 presupposes the existence of a family".[917]

Article 12 UDHR and 17 ICCPR support a similar interpretation. Article 12 UDHR includes both negative and positive state obligations,[918] the latter being implicit in the formulation of the second paragraph.[919] Article 17 ICCPR is interpreted by the Human Rights Committee (hereafter HRC)[920] in a similar vein, in an acknowledgement that attacks upon privacy can come from very different sources.[921] According to Scheinin, paragraph one of article 17 ICCPR envisages "a negative state obligation *not to violate* privacy rights (paragraph 1) and a positive obligation to *ensure* (protect) the same rights (including in respect of attacks by third parties)"[922] whether those individuals are "in the territory of a State Party, or (otherwise) subject to their jurisdiction".[923] Paragraph two of article 17 ICCPR distinguishes between "plain (and presumably permissible) '*interference'* and actual *violations* of the right – characterised as *arbitrary* interference, *unlawful* interference or *unlawful* attacks".[924] It substantiates into a positive obligation to ensure that the prohibition of such interferences is enforced, and to legislate, whenever State Parties have effective control over the territory.[925]

Articles 12 UDHR and 17 ICCPR also address interferences that are horizontal, i.e. committed by natural and legal persons. However, most claims brought under article 17 ICCPR are directed against the state, which is nevertheless under no obligation to reinstate a condition of private life that has been impaired.[926]

Article 8 ECHR, by contrast, works only vertically, but is capable of producing some sort of horizontal indirect effects. While cases of violations by private actors cannot be

[915] Ibid.
[916] Marckx v. Belgium, n. 6833/74, CE:ECHR:1979:0613JUD000683374, para 31.
[917] Ibid.
[918] Rehof (1995).
[919] Morsink (1999).
[920] Human Rights Committee (CCPR) (1988).
[921] Nowak (2005 (2nd edition)).
[922] Martin Scheinin, *Written testimony related to the surveillance program conducted under Section 702 of the FISA Amendments Act* (2014) 2.
[923] Ibid, p. 4.
[924] Ibid, p. 2.
[925] Ibid.
[926] Nowak (2005 (2nd edition)).

brought before the ECtHR, states may face "positive obligations inherent in an effective respect for private or family life ... These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves",[927] and the case law of the ECtHR can be cited in national cases.[928] Some scholars have pointed to the fact that the provisions of the Charter are likely to trigger, at a minimum, horizontal indirect effects.[929] It will be for the CJEU to determine the effects produced by article 7 of the Charter, and envisage a higher level of protection than article 8 ECHR.

2.2.3 *"His or her private and family life, home and communications", and scope of the right*

As discussed in chapter two (section 3.1), the elusiveness of the term has meant that the many attempts of eminent scholars to define 'privacy' have grasped aspects of the concept, but such attempts have not proved conclusive. Courts are no different. Bygrave acknowledges that article 8 ECHR has been "one of the most frequently contested rights in case law pursuant to the Convention".[930] On the one hand, Courts have consistently, and openly, avoided providing strict definitions of the right (see chapter 5, section 1). As a result it has been difficult to identify the essence of the right, which weakens the imposition of clear and strict permissible limitations existing in *leges generales* and *speciales*. On the other hand, such avoidance has left open the possibility to extend the scope of the application of the right *vis-à-vis* societal changes. In fact, the ECtHR, under the 'living instrument' doctrine, has adopted an evolutive interpretation in line with present-day conditions (including social, technological and cultural developments).[931] As a result, there is no "ready-made" definition of situations falling *a priori* within the scope of the four limbs of the right.[932]

When it comes to the limbs, it should be first noted that Article 7 of the Charter, like article 8 ECHR, does not explicitly protect honour and reputation (which however surface in

[927] X and Y v. the Netherlands, n. 8978/80, CE:ECHR:1985:0326JUD000897880, para 23.
[928] Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action' in Yves Poullet Serge Gutwirth, Paul De Hert, Sjaak Nouwt and Cécile de Terwangne (ed), *Reinventing Data Protection?* (Springer 2009).
[929] Craig (2013).
[930] Bygrave (2014), p. 6.
[931] See, in the context of family life, *X and Y v. the Netherlands, no. 8978/80*, para 139.
[932] Zeno-Zencovich (2001).

case law relating to identity, see *infra,* section 3.3.1.). The *travaux préparatoires* of article 8 ECHR clarify that the exclusion of attacks against honour and reputation was intentional,[933] and paved the way to the protection of freedom of expression, enshrined in article 10 ECHR.[934] This might have been a consequence of the discussions which occurred around article 12 UDHR. Not only was the inclusion of the terms 'reputation' and 'honour'[935] widely debated due to the risks of abuse and curbing free speech and freedom of the press,[936] but such inclusion also determined the decision to forgo the adjective 'inviolable', despite many constitutions referring to private life as such, as the word did not attach well to reputation and honour.[937] Article 17 ICCPR offers lower protection to honour and reputation than the other interests enshrined in the article,[938] as the threshold for infringing freedom of expression[939] is higher ("unlawful attacks").[940]

The limbs protected by article 7 of the Charter are the same as those protected by article 8 ECHR, with the exception of the term 'communications', used instead of 'correspondence',[941] to reflect the technological evolution occurred in the past 60 years.

Thus far, the limbs of the right have featured in fewer than 100 judgments of the CJEU, mostly on private and family life, and also on communications. The CJEU provided either an autonomous interpretation, or referred to the case law of the ECHR by analogy. The CJEU can rely on more than 6000 cases on article 8 ECHR dealt with by the Strasbourg court. Luxembourg's scant cases on article 7 would pale by comparison with those by the ECtHR if it were not for the young age of the Charter. However, it is important to pause on the quantitative element, whose practical consequence is not only that the Strasbourg case law is more detailed, but also broader than that on article 7 of the Charter. The ECtHR has been using article 8 in an expansive way, to provide protection in situations that would not be otherwise covered by the Convention. Hence, the clause has given protection to the right to a name, physical integrity in a broad sense,[942] collective health protection, home, all forms of communications, processing of personal data, sexual life, family in a wide sense (including

[933] Council of Europe (1956).
[934] Zeno-Zencovich (2001).
[935] Morsink (1999).
[936] Rehof (1995).
[937] Morsink (1999).
[938] Nowak (2005 (2nd edition)).
[939] The burden of proof of the unlawfulness of attacks against honour and reputation is on the plaintiff, in order to safeguard the potentially competing right of freedom of expression (Simons v. Panama 460/91 and I.P. v. Finland 450/91 in Blair (2005)).
[940] Council of Europe (1956).
[941] To this effect, see *C-400/10 PPU - McB*, para 53.
[942] Rehof (1995).

parent-child relationship, immigration and expulsion and minors entrusted to other families), and protection of the environment.[943] In a similar vein, article 17 ICCPR[944] embraces wide definitions of the limbs, though not as comprehensive as those given to article 8 ECHR.

The mismatch between the purview of article 8 ECHR and of article 7 of the Charter is particularly relevant for the discussion of the attributes, to which I move now.

3 ATTRIBUTES OF ARTICLE 7 OF THE CHARTER

This section illustrates the attributes of **the right to respect for private and family life, based on the** Human Rights Measurement Framework (hereafter HRMF) study. Since the HRMF takes as a reference article 8 ECHR, its findings need revising in the light of EU applicable law. I first describe the HRMF, then discuss the changes needed due to the difference in scope between article 8 ECHR and 7 of the Charter, and sketch the content of the attributes based on EU case law, ECtHR case law, and instruments of international law that supply guidelines – if and when relevant.

3.1 THE HUMAN RIGHTS MEASUREMENT FRAMEWORK (HRMF)

An identification of the attributes of the right to respect for private and family life can be found in the HRMF realized by the Equality and Human Rights Commission (hereafter EHRC). The HRMF is "conceptually anchored"[945] in the study conducted by the OHCHR discussed in chapter 5 (section 3.3). Both aim to build indicators to promote the incorporation of human rights into policies and foster a culture of respect for human rights, rather than identify violations.[946] This thesis does not develop indicators (on the potential to do so, see concluding chapter); yet the HRMF is an authoritative source for the attributes of the right to

[943] Zeno-Zencovich (2001).
[944] Human Rights Committee (CCPR) (1988); Nowak (2005 (2nd edition)); Blair (2005).
[945] Candler and others (2011), p. 16.
[946] The HRMF borrows from the OHCHR study the concept of attributes and the three-layered indicators, namely structural indicators (the commitment to human rights standards in principle), process indicators (the effort effectively made to implement such standards) and outcome indicators (the results of such efforts in practice).

respect for private and family life, both because of the body issuing it (the EHRC), and because the attributes and indicators were validated by consultations with stakeholders.

The HRMF adapted the OHCHR's methodology to better reflect the specificities of the United Kingdom, namely its legal framework of reference and the bodies entrusted with overseeing the enforcement of human rights. In particular, the HRMF identifies relevant attributes primarily against the Human Rights Act, which is the legal instrument that incorporated into UK domestic law the ECHR and made the rights enshrined therein fully enforceable. Moreover, the HRMF relied on rights set out in international agreements ratified by the UK, but which are not necessarily enforceable (a difference which was stressed in many respects). The Charter is, surprisingly, not mentioned.

Accordingly, the indicators relating to the right to respect for private and family life[947] (dashboard 41-50) enable us to measure results on the following attributes (for the UK legal context):

- Private life
  - Physical and psychological integrity;
  - Personal social and sexual identity;
  - Personal development, autonomy and participation;
- Personal information and surveillance (hence the protection of personal data is incorporated in the right to respect for private and family life).
- Correspondence;
- Family life;
- Home;
- Environmental rights.

3.2 REVISING THE HRMF ATTRIBUTES IN THE LIGHT OF THE CHARTER

Due to its jurisdiction-specificity, and the absence of references to EU law, the attributes elaborated by the HRMF need to be revised in accordance with the Charter. The point of such exercise is to attain the purpose of attributes as described in chapter 3, i.e. to

[947] The 2011 study contained a dashboard of 10 indicators on "The Right to Respect for Private and Family Life" derived from article 8 ECHR: Indicator 41: Legal and constitutional framework; Indicator 42: Legal precedents, gaps and standard-setting; Indicator 43: Regulatory framework; Indicator 44: Public policy framework; Indicator 45: Outcomes of key judicial, regulatory and investigative processes; Indicator 46: Privacy, identity and autonomy; Indicator 47: Spotlight statistics: The detention context; Indicator 48: Spotlight statistics: Unmet basic needs that may meet the Article 8 threshold; Indicator 49: Spotlight statistics: Abuse, neglect, discrimination, lack of dignity and respect; and Indicator 50: Spotlight statistics: Public attitudes, understanding and experiences." (p. xxxvii)).

reach a limited number of characteristics that are unique to that right, and that do not overlap, internally and externally. The purpose is not rebutting the clear overlap between different rights, but to acknowledge such overlap in order to delimit the scope of each right.[948] Revisions relate primarily to four points.

First, since, (as I detail in chapters 2 and 7,) I argue that the right to the respect of private and family life and the right to the protection of personal data should be kept distinct, 'personal information' should not form part of the attributes of private life.

Here I wish to rebut the potential criticism that the ECJ has often failed to trace a strong distinction between the two rights. As noted in chapter 1, the Court is bound to interpret existing legislation and the language therein. Part of the problem may have to do with the scope of Directive 95/46/EC, which refers to the "right to privacy with respect to the processing of personal data".

The text of the General Regulation on Personal Data Protection may provide an important solution to the problem. Article 1 of the Regulation in its adopted version reads "this Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data" and "… protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data". Likewise, recital one of the Regulation does not contain references to the ECHR or private life: "The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty lay down that everyone has the right to the protection of personal data concerning him or her."

Secondly, having excluded personal information from the scope of article 7 of the Charter, it seems apt to discuss the destiny of the orphaned 'surveillance'. Surveillance embodies the antipode of secrecy, to which unfortunately 'privacy' is often equated[949] (chapter 2, section 3.3.1.1 and chapter 7). In between such extremes lie confidential communications and (lawful) interception, the object of article 7 as discussed in section 4. To be sure, surveillance is not a component of private life, being as it is capable of affecting

[948] It is appropriate to recall the original use of attributes, briefly mentioned in chapter 5, section 3.4, which I also describe in Porcedda (2013), *Paper Establishing Classification of Technologies on the Basis of their Intrusiveness into Fundamental Rights* (SURVEILLE Project Deliverable D2.4). There, the purpose of attributes was to highlight trees of intrusions into fundamental rights. In a hypothetical study including all articles of the Charter, the dimensions currently excluded from article 7 would be reconsidered as part of other articles (e.g., in the present case, articles 3, 8 and 37 of the Charter). Hence, their exclusion from the present discussion does not imply their irrelevance *tout court*, but simply for the article at stake, with a view to identifying attributes that are unique to it.

[949] Solove (2011), *Nothing to hide*; Westin (1967).

personal data (as the original formulation 'personal information and surveillance' suggests). Hence, I would drop this entirely. Conversely, correspondence, in line with the language of article 7, becomes 'communications'.

Thirdly, the attribute 'environmental protection' can be dropped as a result of the homonymous article 37 of the Charter, which states that a high level of environmental protection and the improvement of the quality of the environment must be integrated into the policies of the Union and ensured in accordance with the principle of sustainable development. Such interpretation is supported by a recent case, *Commission v. Austria*,[950] which concerns the failure of the Republic of Austria to fulfil its obligations under Articles 28 EC and 29 EC as a consequence of prohibiting lorries of over 7.5 tonnes carrying certain goods from using a section of the A 12 motorway in the Inn valley (Austria). One of the arguments presented by Austria to justify its decision was the "protection of health and the environment and…the need to ensure respect for private and family life enshrined in Article 7 of the Charter and Article 8(2)" ECHR.[951] In appraising the argument of the Republic of Austria, the ECJ recalled that

> *"The protection of health and the protection of the environment are essential objectives of the European Union. Article 2 EC states that the Community has, as one of its tasks, to promote 'a high level of protection and improvement of the quality of the environment' and Article 3(1)(p) EC states that the activities of the Community are to include a contribution to the attainment of 'a high level of health protection'. The transversal and fundamental nature of those objectives is also reaffirmed in Articles 37 and 35 respectively of the Charter. As to the relationship between the objectives of protection of the environment and protection of health, it is apparent from Article 174(1) EC that the protection of human health is one of the objectives of Community policy on the environment..."*.[952]

In other words, the Court did not refer to article 7 of the Charter or 8 ECHR, but rather to the specific articles of the Charter, which it is subsequently necessary to treat as separate rights.

Finally, the sub-attribute 'Physical and psychological integrity' has to be revised in the light of article 3 of the Charter, entitled 'right of the integrity of the person', which reads:

[950] Judgment of 21 December 2011 in Commission v. Austria, C-28/09, EU:C:2011:854.
[951] Ibid, para 118.
[952] Ibid, paras 120 -122.

"Everyone has the right to respect for his or her physical and mental integrity. 2. In the fields of medicine and biology, the following must be respected in particular: (a) the free and informed consent of the person concerned, according to the procedures laid down by law; (b) the prohibition of eugenic practices, in particular those aiming at the selection of persons; (c) the prohibition on making the human body and its parts as such a source of financial gain; (d) the prohibition of the reproductive cloning of human beings."

As a result, the attributes of article 7 of the Charter should exclude the principles pertaining to article 3 of the Charter, which, according to the Explanations, "are already included in the Convention on Human Rights and Biomedicine, adopted by the Council of Europe (ETS 164 and additional protocol ETS 168)", and which, in the case law of the ECtHR, fall within the remit of article 8 ECHR.[953] Although the scant case law on the subject matter provides little insight, the recent case of *A, B, and C*[954] could provide some guidance. The preliminary ruling request was made in proceedings between A, B and C, who are third country nationals, and the Dutch State Secretary for Security and Justice, concerning the rejection of their applications for temporary residence permits (asylum) in the Netherlands on grounds of homosexuality. Dutch authorities had rejected previous requests as they alleged the applicants had not substantiated their claims, or were not credible. The referring court asked the extent to which detailed questioning as to the sexual practices of an applicant for asylum, and 'tests' with a view to establishing his homosexuality, carried out pursuant to article 4 of Directive 2004/83/EC on minimum standards for the qualification of refugees, was compatible with fundamental rights as protected by the Charter.

While the ECJ (Grand Chamber) followed the reasoning of the Advocate General, the Court did so by relying on articles 1 and 7 of the Charter, rather than articles 3 and 7 of the Charter as Advocate Sharpston had done.[955] Even if the choice of the ECJ does not firmly define the relationship between the two rights, Advocate Sharpston's views allow drawing some interim conclusions. She found that asking explicit questions concerning an applicant's sexual activities and proclivities to be violating both articles 3 and 7 of the Charter, the first because of their content of a medical nature (while noting that homosexuality is not a medical or psychological condition), the second because of its intrusiveness.[956] Article 3 would thus cover the performance of medical activities, whereas article 7 would deal with the

[953] See the case of Glass v. UK no. 61827/00, CE:ECHR:2004:0309JUD006182700, mentioned in Candler and others (2011).
[954] Judgment of 2 December 2014 in A, B, and C, Joined cases C-148/13 to C-150/13, EU:C:2014:2406.
[955] Opinion of Advocate General Sharpston of 17 July 2014 in A, B and C, Joined Cases C-148/13, C-149/13 and C-150/13, EU:C:2014:2111.
[956] Ibid, paras 60-63 and 67.

consequence for the mind, body and life of individuals.

3.3 THE ATTRIBUTES IN THE EU LEGAL FRAMEWORK

The result of the revision of the HRMF attributes leads to the following reformulation:

- Private life
    - Physical and psychological integrity (excluding in the context of medicine and biology)
    - Personal social and sexual identity
    - Personal development, autonomy and participation
- (Confidential) communications
- Family life
- Home

In what follows I sketch the content of the attributes by referring to the interpretation of the CJEU and the ECHR, but also, when relevant, of the HRC as discussed by scholarship. I describe the attributes in positive terms, whereas I address interferences in section four on permissible limitations. Each sub-paragraph contains a discussion of the essence of the right pursuant to article 52 (1) of the Charter. Due to the scant case law of the CJEU on the matter, I attempt to identify the core in relation to most attributes, under the understanding that such an exercise is speculative and experimental.

3.3.1 PRIVATE LIFE

The CJEU has yet to define the concept of private life, possibly in keeping with the reasoning of the ECtHR, which "does not consider it possible or necessary to attempt an exhaustive definition of the notion".[957] I explained the reasons for my agreement with such an approach in chapter 1. Suffice to recall here that such indeterminacy is linked with the importance of private life in the development of identity,[958] which is subjective and evolves

[957] *Niemietz v. Germany, n. 13710/88*, para 29.
[958] In A.R. Coeriel et al. v. the Netherlands (453/91), the HCR clarified that privacy "refers to the sphere of a person's life in which he or she can freely express his or her identity, be it by entering into a relationship with

with time(s). A clear example is offered by the case law concerning sexual orientation discussed later in this section.

The ECJ has held that the notion of private life includes activities of a professional nature,[959] following the ECtHR, which said, *inter alia* in *Niemietz*, that "it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that…it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not".[960]

According to the General Court, the notion of private life includes the personal financial situation, including pension contributions,[961] and, *a contrario*, the availability of one's funds.[962] In line with the overlap between article 7 and 8 described in chapter 1, information about one's life forms part and parcel of private life,[963] which is endangered when such information is freely made available to third parties. However, when the ECJ said in *YS and Others* that the notion of private life "means, *inter alia*, that that person may be certain that the personal data concerning him are correct and that they are processed in a lawful manner",[964] it did so *per incuriam*, mixing article 7 with article 8 of the Charter.

Thus far, the CJEU has openly relied on the case law of the ECtHR, which has effectively summarized the various facets of private life as follows:

> *"The concept of "private life…covers the physical and psychological integrity of a person...aspects of an individual's physical and social identity...gender identification, name and sexual orientation and sexual life...personal development…relationships with other human beings and the outside world…personal autonomy."*[965]

This passage synthetically introduces the three sub-attributes of private life, to which I move now.

---

others, or alone" in Blair (2005), p. 79. On this point, see also Nowak, for whom privacy underpins the idea of individual existence, and hence identity. This includes one's name, appearance, clothing, hair and beard style, gender, genetic code, feelings and thoughts, one's specific past (Monaco vs. Argentina), religions and beliefs. Nowak (2005 (2nd edition)).

[959] Judgment of 9 November 2010 in Schecke and Eifert, C-92/09 and C-93/09, EU:C:2010:662, para 59.

[960] *Niemietz v. Germany, n. 13710/88*, para 29.

[961] Judgement of 15 July 2015 in Dennekamp v. Parliament, T-115/13, EU:T:2015:497, para 44.

[962] *T-202/12 - Al Assad v. Council*, para 115.

[963] *C-518/07 - Commission v. Germany*, para 21. *Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*, paras 34-35.

[964] Judgment of 17 July 2014 in YS and others, Joined cases C-141/12 and C-372/12, EU:C:2014:2081, para 44.

[965] *Pretty v. the United Kingdom, n. 2346/02*, para 61. See case law cited.

3.3.1.1 Physical and psychological integrity (excluding in the context of medicine and biology)

Besides a reference in passing to "privacy or the integrity of the individual",[966] the ECJ touched upon matters of physical and psychological integrity in *Schwarz*,[967] where it held that "…taking two fingerprints is not an operation of an intimate nature…nor does it cause any particular physical or mental discomfort" and "The combination of two operations designed to identify persons may not *a priori* be regarded as giving rise in itself to a greater threat to the right(s)" to private life. It is unfortunate that the Court missed the chance to elaborate on the matter of integrity *vis-à-vis* an exposure of bodily parts.

The ECtHR has also touched upon the matter in general terms in *Pretty v. UK*, where it held that article 8 "covers the physical and psychological integrity of the person".[968] The increasing availability of techniques and technology capable of exposing the body and the mind may trigger more case law in the future.

In the interim, this attribute can be described as the combination of the *forum internum* of the mind and the *forum internum* and *externum* of the body. The former concerns unspoken thoughts, feelings and emotions.[969] Once considered the most inaccessible part of the individual, advances in neuroscience and brain imaging are challenging this assumption.

As for the body, the *forum internum* concerns genetic characteristics and unique physical traits that cannot be replicated, while the *forum externum* concerns "the right to own one's body, which also comprises a right to act in a manner injurious to one's health, including committing suicide".[970] It also means control of and resistance to undesired or forced access to one's body, as is the case of intrusive body searches,[971] body scanning, corporal sanctions[972] and sexual violence (which partly overlaps with sexual identity). In cases

[966] Judgment of 29 June 2010 in Bavarian Lager Ltd, C-28/08 P, EU:C:2010:378, para 58.
[967] *C-291/12 - Schwarz*, paras 48-49.
[968] *Pretty v. the United Kingdom, n. 2346/02*, para 61.
[969] To this effect, see also Rachel L. Finn, David Wright and Michael Friedewald, 'Seven Types of Privacy' in Ronald Leenes, Serge Gutwirth, Paul de Hert, and Yves Poullet (eds), *European Data Protection: Coming of Age* (Springer 2013).
[970] Nowak (2005 (2nd edition)), p. 389. However, such autonomy is often deemed contrary to the common good and has paved the way to a number of decisions imposing (or prohibiting) certain acts, such as wearing safety belts: Singh Bhinder v. Canada, Communication n. 208/1986, CCPR/C/37/D/208/1986.
[971] The HRC stated that personal body searches must respect the dignity of the searched, and be performed by a person of the same sex, Human Rights Committee (CCPR) (1988). The practice of strip-searching was for instance deemed arbitrary in the presence of alternative, less intrusive methods (United Nations, Human Rights Committee, *Comments of the Human Rights Committee: United Kingdom of Great Britain and Northern Ireland* (CCPR/C/79/Add 55, 1979) in Blair (2005).
[972] Discussing ECtHR Costello-Roberts v. United Kingdom, Zeno-Zencovich (2001).

of rape,[973] the ECtHR stated that "fundamental values and essential aspects of private life are at stake",[974] and found a violation of article 8 ECHR.

***

Thus far, there is no case law discussing the **essence** of this limb. In the interim, the *forum internum* of the mind and body can be considered good candidates, in that they represent, respectively, the seat of one's personality, and one's unique traits.

3.3.1.2 Personal social and sexual identity

The notion of identity is composite and relates to the way in which an individual portrays herself, or is portrayed, to the external world. The need to display a unified and dignified identity and personality, so crucial in life in society as discussed in chapter 1, corresponds to the *forum externum* of mental integrity.

Similarly to the notion of 'private life', Courts do not define the meaning of identity. In *A, B, and C* (discussed *supra,* section 3.2), while acknowledging the usefulness of standardized tools of assessment, the ECJ stated that relying solely on stereotyped notions of homosexuality is not sufficient to grant the status of refugee, since it is necessary to "take account of the individual situation and personal circumstances of the applicant",[975] and decided in fact that reliance on stereotyped notions is precluded by EU law. This passage provides a small, yet significant reference to the unique nature of identities, and the need to acknowledge this.

A useful indication of the relevance of this attribute comes from the ECtHR, which stated "private life requires that everyone should be able to establish details of their identity as individual human beings and that an individual's entitlement to such information is of importance because of its formative implications for his or her personality".[976]

Cases on identity/personality typically concern three issues: one's name as the first identifier, one's sexual orientation, and one's reputation.

On names, the CJEU stated that a person's name,[977] forename and surname[978] are "a constituent element" of one's identity and private life, "the protection of which is enshrined in

[973] E.g. abuse of a mentally ill woman in *X and Y v. the Netherlands, no. 8978/80*. E.g. abuse of a 14 year old girl in *M. C. v. Bulgaria, n. 39272/98, CE:ECHR:2003:1204JUD003927298.*
[974] *M. C. v. Bulgaria, n. 39272/98*, para 150.
[975] *Joined cases C-148/13 to C-150/13 - A, B, and C*, para 62.
[976] Mikulić v. Croatia, n. 53176/99, CE:ECHR:2002:0207JUD005317699, para 54.
[977] *C-208/09 - Sayn-Wittgenstein*, para 52.

Article 7 of the Charter … and in Article 8 of the [ECHR]. Even though Article 8 of that convention does not refer to it explicitly, a person's name, as a means of personal identification and a link to a family, none the less concerns his or her private and family life".[979] Hence, individuals have a right "to protection of …identity and private life" and "…the way in which [States decide to structure the name requirements in an official document] must observe that individual's right to protection of his private life." For the court, it is apparent that "where the name of a person appears incorrectly or ambiguously in documents issued by a State in order to prove his identity, this is liable to cause serious inconvenience for that person both in his professional and in his private life in so far as it may give rise to doubts as to his real identity, the authenticity of the passport or the veracity of the information contained in it".[980] Such inconvenience is liable to cause reputational damage, as discussed below. The ECtHR has recognized the particularly sensitive nature of the name in the case of transsexual and transgender individuals.[981] Likewise, article 17 ICCPR protects one's choice of a surname.[982]

The social reflection of one's identity is fundamental for life in community (and the next attribute), and its deterioration can have dire effects on participation in society and one's well being. Although, as discussed *supra* (section 2.2.3), honour and reputation are not limbs of article 8 ECHR and 7 of the Charter, social identity is a matter of reputation, and the matter has often surfaced in relation to private life. In name cases such as *Sayn-Wittgenstein* and *Runevič*, the Court said that the lack of recognition of one's name may entail "having to dispel suspicion of false declaration caused by the divergence"[983] between different versions of the same name. In *Schecke and Eifert*, publication on a website of data naming the applicants as recipients of public funds and reporting the precise amount received affects their private life[984] because it impacts on their social identity, since anyone can access that information and draw conclusions on the matter. Similarly, in *Google Spain*, the wide availability on the Web of information on Mr Costeja's past insolvency is likely to stain his social identity, and hence affects his private life.[985]

---

[978] *C-391/09 - Runevič-Vardyn*, para 66.
[979] *C-208/09 - Sayn-Wittgenstein*, para 52.
[980] Judgment of 2 October 2024 in U, C-101/13, EU:C:2014:2249, paras 48-50.
[981] Dicussing Res v. United Kingdom, Cossey v. United Kingdom and B. v. France, Zeno-Zencovich (2001).
[982] In A. R. Coeriel et al v. The Netherlands (543/91) as discussed in Blair (2005).
[983] Judgment in *C-208/09 - Sayn-Wittgenstein*, para 68. See, similarly in *C-391/09 - Runevič-Vardyn*, para 78. However, the court upheld the choice of Austria to remove the noble appellative from Ms. Sayn-Wittgenstein's surname on grounds of public policy, namely equality and non-discrimination as understood in Austria.
[984] *C-92/09 and C-93/09 - Schecke and Eifert*, para 58.
[985] *C-131/12 - Google Spain and Google*, para 98.

Such a stain can be intolerable in the case of restrictive measures for terrorism, due to "the opprobrium and suspicion that accompany the public designation of the persons covered as being associated with a terrorist organisation".[986] In this case, public recognition of the illegality of the association with terrorism was fundamental for rehabilitating Mr Ayadi "or constituting a form of reparation for the non-material harm which he has suffered by reason of that illegality".[987] The HRC went in a similar direction in *Sayadi and Vinck*,[988] where it deemed that the dissemination of the United Nations Security Council's terrorist list containing full contact details about the applicants constituted an attack on their honour and reputation, in view of the negative association that some persons could make between the applicants' names and the title of the sanctions list.[989]

Sexual orientation has been the object of evolving case law in recent decades. As Advocate General Sharpston noted, "within the European Union, homosexuality is no longer considered to be a medical or psychological condition".[990] In the words of the ECJ "it is common ground that a person's sexual orientation is a characteristic *so fundamental* to his identity that he should not be forced to renounce it"[991] or to conceal it, whether alone or in a group.[992] The language used by the Court seems to suggest that one's sexual orientation is a core area of the right to private life, though the following passage engenders some ambiguity "…it is unnecessary to distinguish acts that interfere with the core areas of the expression of sexual orientation, even assuming it were possible to identify them, from acts which do not affect those purported core areas…".[993]

Respect for sexual orientation means being free from the threat of imprisonment for one's homosexuality,[994] and not being submitted to detailed questioning as to sexual practices, due to their sensitive nature and importance to identity.[995] The absence of a law criminalizing homosexuality (in extra EU countries) is not deemed a necessary condition for the enjoyment of one's sexual identity; conversely, the ECtHR (and the HRC[996]) has stated that the mere

---

[986] *C-183/12 P - Ayadi*, para 68.
[987] Ibid, para 70.
[988] *Sayadi and Vinck v. Belgium, Communication n. 1472/2006*.
[989] Moreover, one's social identity can be affected also by constantly being referred to as insane when medical reports prove the opposite, e.g. HRC, Birhashwirwa et al. v. Zaire no. 242/87, in Blair (2005).
[990] *Joined Cases C-148/13 to C-150/13, Opinion of Advocate Sharpston* para 60.
[991] Emphasis mine, Judgment of 7 November 2013 in X and Others, Joined Cases C-199/12 to C-201/12, EU:C:2013:720, para 46.
[992] Ibid, para 70.
[993] Ibid, para 78.
[994] Ibid, para 57.
[995] *Joined cases C-148/13 to C-150/13 - A, B, and C*.
[996] In Toonen v. Australia 488/92, article 17 ICCPRS also protects adults' consensual sexual activity in private (Concluding Comments on United Republic of Tanzania 1999 UN doc. CCPR/C/79/Add. 97), in Blair (2005).

existence of a norm criminalising certain sexual behaviour, even if not enforced, constitutes an interference with private life.[997]

***

In cases relating to this sub-attribute, the Court has not explicitly identified what constitutes the **essence**. Some cases, however, provide useful indications. As noted above, the reference in *X and Others*[998] to one's sexual orientation as a "characteristic *so fundamental* to one's identity", makes this element a good candidate for the essence, mindful of the fact that it may not be possible to identify core areas of expression of one's sexual orientation. Likewise, a potential candidate for the essence is the recognition of one's original or acquired name, so long as it does not conflict with imperative needs of *ordre public*. As for cases concerning the social reflection of one's identity, the essence could be defined more in terms of avoiding offensive misrepresentations of the person, i.e. a faithful representation of one's persona.

3.3.1.3 Personal development, autonomy and participation ('the outer circle')

This attribute stems from previous ones. As discussed in chapter 2 (section 3), the respect of one's uniqueness and identity is a precondition to free development, autonomy and participation. In turn, the enjoyment of this attribute requires the absence of regimentation, constriction or monitoring by other parties, particularly the state.

The CJEU has not delved yet into the matter insofar as article 7 of the Charter is concerned. Some passages of *Digital Rights Ireland* could be read as an indirect acknowledgment of this dimension of the right to private life. The Court stated that the information collected through the Data Retention Directive "taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them".[999] This, and the fact that individuals have no control over the way such information is and can be subsequently used "is likely to generate

[997] Discussing the cases of Dudgeon v. United Kingdom, Norris v. Ireland, and Modinos v. Cyprus, ibid.
[998] *Joined Cases C-199/12 to C-201/12 - X and Others*.
[999] *Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*, para 27.

in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[1000]

The ECJ does not draw conclusions, but refers widely to the ECtHR case law on interception and measures of secret surveillance that follow (in part) the reasoning in *Klass v. Germany*. There, the ECtHR stated that the existence of secret surveillance unknown to the public, and hence unchallengeable, could reduce article 8 "to a nullity" (§ 36). Moreover, measures of secret surveillance "characterize the police state" (§ 42), a threat that could become true for contracting states "on the ground of defending democracy" (§ 49).[1001]

As Judge Pettiti stated in his concurring opinion on *Malone v. UK* "the mission of the Council of Europe and of its organs is to prevent the establishment of systems and methods that would allow "Big Brother" to become master of the citizen's private life."[1002] Hence, enjoying private life in a democratic society is substantiated in the freedom to be autonomous and participate without the constant control of the state.[1003] The attribute under analysis is instrumental to the nexus between democracy and private life.

According to the ECtHR, "although no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees" including "a right to personal development".[1004] It furthermore entails (to a certain degree) "the right to establish and develop relationships with other human beings" as "it would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle".[1005] Such a "zone of interaction of a person with others" attracts the protection of article 8 ECHR "even in a public context",[1006] as discussed further in the context of communications. Following the metaphor of the ECtHR on the 'inner circle', the development of social relations represents the 'outer circle', and is the precondition for participation.

***

[1000] Ibid, para 37.
[1001] Klass and others v. Germany, n. 5029/71, CE:ECHR:1978:0906JUD000502971.
[1002] Judge Pettiti, concurring opinion in Malone v. the United Kingdom, n. 8691/79, CE:ECHR:1985:0426JUD000869179.
[1003] As the Court stated in the 'Belgian Linguistic' case, the object of the Article is "essentially" that of protecting the individual against arbitrary interference by the public authorities. *Marckx v. Belgium, n. 6833/74*, para 31.
[1004] *Pretty v. the United Kingdom, n. 2346/02*, para 61.
[1005] *Niemietz v. Germany, n. 13710/88*, para 29.
[1006] Peck v. the United Kingdom, n. 44647/98, CE:ECHR:2003:0128JUD004464798, para 57.

The CJEU has not pronounced itself on the question of the **essence** in relation to this limb of private life. It may be useful to start by noting that the violation of this limb is represented by surveillance (understood as an unlawful interference) and regimentation. Hence, a very preliminary attempt to identify the essence may lead to a result in the negative, in the sense of the absence of secret external constraints.

3.3.2 FAMILY LIFE (THE 'INNER CIRCLE')

Family life represents the 'inner circle' of the individual, that group which predates the existence of the state and which must be respected and protected regardless of "the circumstances in, and time at which, family is constituted".[1007] Similarly to cases concerning sexual orientation, (ECtHR) judgments on family evolved in line with social change

> *"…The State, in its choice of means designed to protect the family and secure respect for family life as required by Article 8, must necessarily take into account developments in society and changes in the perception of social, civil-status and relational issues, including the fact that there is not just one way or one choice when it comes to leading one's family or private life".*[1008]

As seen in chapter 2 (section 3.3.1.3), protection of the family has been instrumental in eliminating "obstacles to the exercise of the fundamental freedoms guaranteed by the Treaty".[1009] The CJEU also noted the negative impact of certain policies on family life, for instance the freezing of funds.[1010] The ECJ adjudicated on family issues also in the context of cooperation in civil matters. There, it has ruled that the determination of what constitutes 'family environment' can be linked with the concept of habitual residence.[1011] The ECJ has also ruled on the family rights of the natural mother and father, and stated that there can be a difference between entitlements. Hence, the fact that, "unlike the mother,[1012] the natural father is not a person who automatically possesses rights of custody in respect of his child … does

---

[1007] *C-578/08 - Chakroun, para 63.*
[1008] X and Others v. Austria, no 19010/07 CE:ECHR:2013:0219JUD001901007, para 139. In this case, the ICCPR is unlikely to supply guidelines, as family life does not protect the consequences of cohabiting outside of marriage (Hoofdman v. the Netherlands 602/94), nor the prohibition of gay marriage (Joslin et al. v. New Zealand 902/99) Zeno-Zencovich (2001).
[1009] *C-391/09 - Runevič-Vardyn*, para 90.
[1010] *C-183/12 P - Ayadi*, para 68.
[1011] *C-497/10 PPU - Mercredi*, para 56.
[1012] Article 17 ICCPR protects the right of a parent to visit his or her minor children (HRC Fei v. Colombia 514/92 and L.P. Czech Republic 946/00) Blair (2005).

not affect the essence of his right to private and family life."[1013] Rather, the right of the natural father substantiates in being entitled to

> *"apply to the national court with jurisdiction, before the removal, in order to request that rights of custody in respect of his child be awarded to him, which, in such a context, constitutes the very essence of the right of a natural father to a private and family life".*[1014]

This framework is enriched by the case law of the ECtHR. Hence, a family (and each of its members) has equal value irrespective of the degree of legitimacy binding its members,[1015] a distinction which "would not be consonant with the word 'everyone', and this is confirmed by Article 14 [ECHR] with its prohibition, in the enjoyment of the rights and freedoms enshrined in the Convention, of discrimination grounded on 'birth'".[1016] In the case of parent-child relationships, family life results more from the element of continuous care,[1017] and it is the duty of the state to "allow those concerned to lead a normal family life",[1018] particularly to enable "as from the moment of birth the child's integration in his family".[1019] Cohabitation is not a determining factor in assessing the presence or absence of family life, as stated in cases of expulsions and immigration,[1020] and matters of transfers of custody, especially outside the family of origin, have to be carefully assessed.[1021]

Family life also requires the continuity of one's living environment. In *Moustaquim v. Belgium,*[1022] the fact that a young man had lived in Belgium since the age of two and for about twenty years with his family, had returned to Morocco only twice, for holidays, and had received all his schooling in French is a strong indicator of one's family life, which has to be taken into account in questions of deportation.

[1013] *C-400/10 PPU - McB*, para 57.
[1014] Ibid, para 55.
[1015] The Court either considered the factual situation (Abdulaziz et al. v. United Kingdom, no. 9214/80 9473/81 9474/81) or the prospective chance of founding a family (ECtHR Boughanemi v. France, no. 22070/93), in Nowak (2005 (2nd edition)).
[1016] *Marckx v. Belgium, n. 6833/74*, para 31.
[1017] Ibid.
[1018] Ibid.
[1019] Ibid.
[1020] C v. Belgium, n. 21794/93, CE:ECHR:1996:0807JUD002179493, para 25. See also Berrehab v. The Netherlands, n. 10730/84, CE:ECHR:1988:0621JUD001073084, para 21. The HRC found that respect for private life prevents forcing a 13 year old to choose whether to stay in one country alone or to follow the parents when they have been expelled (HRC Bakhtiyari et al. v. Australia 1069/02). Zeno-Zencovich (2001).
[1021] Olsson v. Sweden, n. 13441/87, CE:ECHR:1992:1127JUD001344187. Eriksson v. Sweden, n. 11373/85, CE:ECHR:1989:0622JUD001137385.
[1022] Moustaquim v. Belgium, n. 12313/86, CE:ECHR:1991:0218JUD001231386, paras 45-46.

***

The ECJ openly mentioned the **essence** in *MCB,* in relation to the right of the natural father *vis-à-vis* his child, which is represented by the ability to "apply to the national court with jurisdiction, before the removal, in order to request that rights of custody in respect of his child be awarded to him".[1023] The same case may lead to argue that the essence of a mother's family life *vis-à-vis* one's child could be to enjoy rights of custody. In general, the core of family life may be to be able to carry out continuous care for its members without interruption, and to have such care recognized by third parties. Once more, until the court pronounces clearly on the matter, this interpretation remains purely speculative.

3.3.3 (CONFIDENTIAL) COMMUNICATIONS

This attribute refers to the ability of individuals to choose with whom and how to share information, and the presumption that information shared privately should remain confidential (and not used against the individual), regardless of the means chosen.

The ECJ identified the **essence** in "the content of the electronic communications as such,"[1024] whose respect requires the absence of "legislation permitting the public authorities to have access on a generalised basis"[1025] to such content. The ECJ adjudicated only recently its first case concerning the interception of communications, which, alongside retention, constitutes an obvious interference with this limb of article 7 of the Charter.[1026] In *WebMindLicenses*, the ECJ acknowledges the potential for abuse and arbitrariness of the interception of communications,[1027] in keeping with the copious case law of the ECtHR. The reasons for keeping information confidential in a democratic society are those identified above, *mutatis mutandis*, in relation to surveillance of private life. The monitoring of telecommunications can engender a police state contrary to the aim and objectives of human rights and democracy.

[1023] Emphasis mine, *C-400/10 PPU - McB*, para 55.
[1024] *Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*, para 39.
[1025] *C-362/14 - Schrems*, para 94.
[1026] *C-419/14 - WebMindLicenses*, para 71.
[1027] Ibid, paras 77-78.

In the case law of the ECtHR, protecting correspondence means first of all enabling such correspondence to take place,[1028] and ensuring confidentiality no matter the means of communications: letters, phone calls,[1029] telephone numbers, computers and emails,[1030] use of the internet, [1031] voice recording[1032] and CCTV,[1033] whether at home, in the context of business activities, or in a state of deprivation of liberty.[1034] In the latter case, confidentiality applies in particular to the relationship with one's lawyer.[1035]

In assessing the degree to which confidentiality of communications applies, the ECtHR has made use of the concept of "a person's reasonable expectations as to privacy [as a] significant, yet not conclusive, factor".[1036]

Typically the Court would attach lower protection to communications when individuals have willingly or knowingly made activities and information public, unless such information becomes part of a permanent or systematic record. Here it is important to note the overlap with personal data protection.

3.3.4 HOME

Thus far, the CJEU has not delivered an interpretation of the right to a home in EU law,[1037] as opposed to the case law of the ECHR, and contextually also the HRC (as discussed by scholarship[1038]).

The protection currently afforded to the home is in keeping with the adage that one's home is one's castle, in the light of the social role played by the home. In a recent case concerning eviction, *Stolyarova v. Russia*, the ECtHR reaffirmed that

---

[1028] Golder v. the United Kingdom, n. 4451/70, CE:ECHR:1975:0221JUD000445170, para 43.
[1029] See Halford v. the United Kingdom, n. 20605/92, CE:ECHR:1997:0625JUD002060592, para 44.
[1030] *Copland v. the United Kingdom, n. 62617/00*, para 43.
[1031] KU v. Finland, n. 2872/02, CE:ECHR:2008:1202JUD000287202, para 49.
[1032] PG and JH v. the United Kingdom, n. 44787/98, CE:ECHR:2001:0925JUD004478798, paras 59-60.
[1033] *Peck v. the United Kingdom, n. 44647/98*, paras 57-63.
[1034] Herczegfalvy v. Austria, n. 10533/83, CE:ECHR:1992:0924JUD001053383, para 91.
[1035] *Golder v. the United Kingdom, n. 4451/70*, para 43. In this respect, see also HRC case law, for which respecting prisoners' communications means applying only non-arbitrary censorship and control (Pinkney v. Canada 27/77), and permitting to get in touch with families and friends (Estrella v. Uruguay 74/80). Blair (2005); Nowak (2005 (2nd edition)).
[1036] See, *inter alia*, *P.G. and J.H. v. the United Kingdom, n. 44787/98*, para 57.
[1037] The Court recently referred to the risk for "the consumer, and possibly his family…of losing his dwelling in a forced sale" and to "the right to respect for the home, guaranteed under Article 7 of the Charter", without further comments about the relationship between the two. Order of 16 July 2015 in Sánchez Morcillo and Abril García, C-539/14, EU:C:2015:508, paras 41 and 46.
[1038] Nowak (2005 (2nd edition)); Zeno-Zencovich (2001).

> *"The margin of appreciation in housing matters is narrower when it comes to the rights guaranteed by Article 8 [than it is for those guaranteed by in Article 1 of Protocol No. 1], because Article 8 concerns rights of central importance to the individual's identity, self-determination, physical and moral integrity, maintenance of relationships with others and a settled and secure place in the community".*[1039]

What is being protected is a broad notion of one's private space "covering residential premises" and extending "also to certain professional or business premises [which] includes not only the registered office of a company owned and run by a private individual…but also that of a legal person and its branches and other business premises…".[1040] The protection of the workplace, first established in *Niemietz v. Germany*,[1041] has been adopted by analogy by the CJEU (in the context of private life, as seen *supra*, section 3.3.1).

If someone lost his or her house, the notion of home could protect a tent (but not a car).[1042] The right to a home, however, does neither embody a right to a house, or to property, nor to certain lifestyles.[1043]

Rather, respect for home protects dwellers from unlawful, discriminatory or harassing searches and arrests.[1044] The violation of home is often coupled with that of communications.

***

In the almost complete absence of case law on the subject matter, it is particularly difficult to identify the **essence**. In light of the social and individual function of the (broadly understood) home, the essence may be identified in a minimum zone of physical intimacy, e.g. the bathroom or the bedroom.

[1039] *Stolyarova v. Russia, n. 15711/13*, para 59.
[1040] Bernh Larsen Holding As and Others v. Norway, n. 24117/08, CE:ECHR:2013:0314JUD002411708, para 104.
[1041] *Niemietz v. Germany, n. 13710/88*, para 30.
[1042] Nowak (2005 (2nd edition)); Rehof (1995).
[1043] See Velosa Barreto v. Portugal, Akdivar v. Turkey, Buckley v. United Kingdom, respectively, in Lars Adam Rehof, 'The Universal Declaration of Human Rights: A Commentary' in Gudmundur Alfredsson, Asbjorn Eide, Goran Melander, Lars Adam Rehof and Allan Rosas, with the collaboration of Teresa Swinehart (eds), (Scandinavian University Press 1992).
[1044]See HRC Aumeeruddy Cziffra et al. v. Mauritius 35/78, Coronel et al. v. Colombia 778/97, and García v. Colombia 687/1996, in Zeno-Zencovich (2001).

3.4 SUMMARY OF THE ATTRIBUTES OF ARTICLE 7 OF THE CHARTER

The table below summarizes the attributes of article 7 of the Charter. The first row on the left contains the attribute. The row beneath summarizes the content of the attribute. The last two rows contain a summary of the essence. The first one contains the essence openly identified by the CJEU, whereas the second contains suggestions for core areas that I have identified experimentally.

Attribute	Private life	i.Physical and psychological integrity	ii.Personal social and sexual identity	iii.Personal development, autonomy and participation ('outer circle')	Family	Communications	Home
Description	Private life concerns those elements that are relevant to develop and maintain one's personality and identity, understood as unique and worthy of equal respect.	This sub-attribute includes: • The *forum internum* of the mind, i.e. one's thoughts, feelings and emotions. • The *forum internum* of the body: genetic characteristics and unique physical traits • The *forum externum* of the body: the right to own one's body and protect it from undesired or forced access to it.	This sub-attribute concerns the '*forum externum*' of mental integrity, which substantiates in the coherent portrayal of one's personality and identity to the external world. It includes control over one's name, the upkeep of one's reputation, the expression of one's sexual orientation, but also the manifestation of one's beliefs and personality in the form of attitudes, behaviours and clothing.	This sub-attribute is strongly linked and flows from the previous ones, and is concerned with the partaking of individuals in the democratic society • The development of one's personality in the spirit of self-determination • Autonomy of one's movements and actions • Participation in social and political life as one sees fit All the above require a minimum degree of control, even if conducted in public. The possibility to develop social relations of an amicable or professional nature. In this sense, this sub-attribute concerns the 'outer circle' of one's life and links with the 'inner circle' of one's family.	This attribute concerns the 'inner circle', one's kin by blood and election, which represents the first mode of existence in society and comes before the state. It includes horizontal and vertical relationships regardless of their seal of legitimacy, and is substantiated in emotional and material ties with individuals and surroundings.	This attribute refers to the ability of individuals to choose with whom and how to share information, and the presumption that information shared privately should remain confidential, regardless its content and the mode of communication. This includes the expectation that information shared privately will not be used against the individual.	This attribute refers to one's settled and secure place in the community, where individuals can develop ties of an intimate nature and nurture self-determination, far away from the public gaze and undesired intrusion.
Essence (CJEU)	See sub-attributes		The expression of one's sexual identity		For a father, the possibility to apply for the right to custody	The content of one's communications	
Essence (experimental)	See sub-attributes	The *forum internum* of the mind and of the body	Official recognition of one's original or acquired name; Faithful social representation of one's identity	Absence of secret external constraints	Continuity of relationship of care; Recognition of relationship of care		A minimum zone of physical intimacy

Table 13 Summary of attributes of the right to respect for private and family life

4 PERMISSIBLE LIMITATIONS OF ARTICLE 7 OF THE CHARTER

In chapter five (section 3.4), I discussed the contribution of the test for permissible limitations, enriched by the core-periphery method, to the assessment of the impact of technologies on fundamental rights. The test, elaborated by Scheinin,[1045] was based on the case of the ICCPR. This section describes the permissible limitations applicable specifically to articles 7 and 8 of the Charter,[1046] as a preliminary step for the application of step four of the methodology.

Differently from the ECHR, the Charter does not distinguish between qualified and absolute rights, and it is therefore for the European judge to decide which are qualified rights.[1047] In *Schwarz*, the ECJ clearly stated, "the rights recognised by Articles 7 and 8 of the Charter are not absolute rights, but must be considered in relation to their function in society".[1048] In line with their meaning in other instruments,[1049] privacy rights are subject to permissible limitations, which form the subsequent step of the methodology of appraisal of the impact of cybercrimes on rights. In order to qualify as permissible, interferences or attacks must comply with precise criteria. It is here that the discussion as to whether article 7 of the Charter corresponds to article 8 ECHR is capable of having material consequences. In this respect, I first revise limitations inherent within article 8.2 ECHR (section 4.1), and subsequently analyse limitations stemming from article 52 of the Charter (section 4.2).

4.1 LIMITATIONS IN THE LIGHT OF ARTICLE 8.2 ECHR

As discussed *supra* (section 2), insofar as article 7 corresponds to article 8 ECHR, the meaning and scope of the former has to be construed in the light of article 8 ECHR. Pursuant to article 8.2 ECHR, interferences must be

[1045] Scheinin (2009), *Report on Human Rights and Fundamental Freedoms while Countering Terrorism*.
[1046] The CJEU has thus far favoured a joint reading of privacy rights in the context of the application of a test for permissible limitations. Article 29 Data Protection Working Party, *Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector* (536/14/EN WP 211, 2014), point 2.1.
[1047] Porcedda, Vermeulen and Scheinin (2013).
[1048] Judgment in *C-291/12 - Schwarz*, para 33.
[1049] Article 8.2 ECHR and articles 17 (and 4) ICCPR (and 12 and 29 UDHR) demonstrate that the right to private and family life is not an absolute right, but it can be interfered with by means of permissible limitations.

"In accordance with the law" and "necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The ECtHR expressed itself extensively on the grounds for permissible limitations, and developed a test based on the criteria of legality and lawfulness ('in accordance with the law'), necessity ('necessary in a democratic society') and proportionality; sometimes 'the pursuit of a legitimate aim is seen as a second ground, followed by necessity (which includes proportionality).[1050]

To begin with, the ECtHR assesses legality, which, as De Hert and Gutwirth[1051] noted, has progressively incorporated several tenets of the rule of law.[1052] Interferences "in accordance with the law" are substantiated in two requirements. First, there must be a legal basis, failing which the interference is impermissible, thus amounting to a violation. In *P.G. and J.H. v. UK*,[1053] multiple violations of article 8 ensued from the absence of a law regulating the use of covert surveillance, particularly "specific statutory or other express legal authority"[1054] proportionate to the invasive measures analyzed in the case. The second requirement is the quality of law. The legal basis must "comply with the requirements laid down by the domestic law providing for the interference"[1055] and must be "accessible to the person concerned, who must moreover be able to foresee its consequences for him, and that it is compatible with the rule of law".[1056]

The objective of the quality of law is to minimize the occurrence of arbitrariness.[1057] This is particularly the case for matters of secret surveillance, where foreseeability cannot entitle an individual to foresee when the covert measure is taking place. In *Iordachi and Others v. Moldova*, confirming the interpretation developed in *Weber and Saravia*, foreseeability substantiates in "clear, detailed rules on interception" allowing citizens "an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures",[1058] clarifying in particular the scope and manner of the exercise of discretion conferred on the competent authorities. With a

[1050] Article 29 Data Protection Working Party (2014), *Opinion 01/2014, WP 211*.
[1051] De Hert and Gutwirth (2009).
[1052] Craig (2013).
[1053] *P.G. and J.H. v. the United Kingdom, n. 44787/98*, paras 37-38, and 63.
[1054] Ibid, para 62.
[1055] Perry v. the United Kingdom, n. 3737/00, CE:ECHR:2003:0717JUD006373700, para 45 and following.
[1056] *P.G. and J.H. v. the United Kingdom, n. 44787/98*, para 44.
[1057] "What is required by way of safeguard will depend, to some extent at least, on the nature and extent of the interference in question." Ibid, para 46.
[1058] Iordachi and Others v. Moldova, n. 25198/02, CE:ECHR:2009:0210JUD002519802, para 39.

view to prevent unfettered power, laws on secret surveillance should therefore include the following minimum safeguards: "the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed".[1059]

If the debated measure satisfies the tenets of the rule of law, then the ECtHR addresses the question as to whether the interference is 'necessary in a democratic society', a question leading to the political issues of the margin of appreciation and balancing. The assessment of the criterion of necessity entails two to three steps. The first consists in evaluating whether the measure responds to a pressing social need:

> *"The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued."*[1060]

De Hert and Gutwirth note, however, that this test is applied often in cases concerning article 10 ECHR, but rarely with regards to article 8 ECHR.[1061]

The second is whether the interference responds to a legitimate aim.[1062] This was the case, for instance, in *Klass v. Germany*:

> *"The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime."*[1063]

If the Court is satisfied that the measure responds to a legitimate aim, it then applies the third step, i.e. the proportionality test. De Hert and Gutwirth identified four steps of the test: i) an analysis of the nature of the measure under discussion, including its reach and potential for abuse; ii) the availability of less intrusive measures, or a less drastic implementation of the measure under discussion; iii) the conditions of the applicant, which could justify different

[1059] Ibid.
[1060] Leander v. Sweden, n. 9248/81, CE:ECHR:1987:0326JUD000924881, para 58.
[1061] As in Handyside v. UK, n. 5493/72, in Porcedda, Vermeulen and Scheinin (2013).
[1062] De Hert and Gutwirth (2009). Where the 'legitimate aim' is seen as a second, independent ground, this equates to the availability of relevant and sufficient reasons. Article 29 Data Protection Working Party (2014), *Opinion 01/2014, WP 211*.
[1063] *Klass and Others v. Germany, n. 5029/71*, para 48.

degrees of limitations, as is the case of people in a state of deprivation of liberty; and iv) the availability of safeguards that counterbalance the intrusiveness of the measure.[1064] For instance, in *Niemietz v. Germany*, the Court found the search of the applicant's lawyer's office was disproportionate to the legitimate aim pursued (insulting and bringing pressure on a judge), because the search warrant was drawn in too broad terms (i-ii), it concerned the office of a lawyer, a profession that entails a greater degree of confidentiality (iii), and the search, in Germany, is usually carried out without special safeguards (iv) (e.g. without independent oversight).[1065]

Hence, insofar as article 7 of the Charter corresponds to article 8 ECHR, the permissibility of an interference should be assessed on the basis of the existence of an adequate legal basis, the legitimacy of the aim pursued by the interference (in a democracy), and the degree of intensity of the interference *vis-à-vis* the aim pursued and the factual circumstances.[1066] As seen in earlier sections of this chapter, since the scope of article 7 of the Charter is narrower than article 8 ECHR, in theory the limitations formulated in the second paragraph should apply *in toto* to article 7 of the Charter. Here, however, theory and practice may differ, paving to the third mismatch, as anticipated *supra*, in section 2.1.1.

4.2 LIMITATIONS INHERENT TO THE CHARTER

In her book, Gonzáles Fuster[1067] questions the correspondence of article 7 of the Charter with article 8 ECHR, based on a comparison of article 8.2 ECHR (quoted at the beginning of this section) and article 52.1 of the Charter, which is the horizontal clause on permissible limitations and reads:

> *"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. 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."*

[1064] De Hert and Gutwirth (2009).
[1065] *Niemietz v. Germany, n. 13710/88*, para 37.
[1066] "The Court's task is not to review the relevant law or practice in the abstract but rather to confine itself, without overlooking the general context, to examining the issues raised by the case before it", *Peck v. the United Kingdom, n. 44647/98*, para 102.
[1067] González Fuster (2014).

The Explanations clarify that limitations must be interpreted restrictively[1068] and cannot "constitute, with regard to the aim pursued, disproportionate and unreasonable interference undermining the very substance of those rights".[1069] The formulation of the article would also allow for the application of a margin of appreciation.

Gonzáles Fuster expresses doubts in relation to the correspondence between: "in accordance with the law" and "provided for by law"; "necessary in a democratic society" and the proportionality principle; and the "legitimate aims" and the "objectives of general interest". The latter may harbour the greatest divisions, as the objectives of general interests of the EU are those contained in articles 2,[1070] 3 and 4(1) TEU, and 35(3), 36 and 346 TFEU, to be understood cumulatively.

She then mentions two further reasons for mismatch, namely the obligation, set out in article 52.1 of the Charter, to respect the essence of the right, and the possibility for the Union law to grant additional protection to the fundamental rights pursuant to article 52.3 of the Charter. These two points may create a permanent mismatch between the protection afforded by the two Courts, and could pave the way to an independent interpretation of the right.

In fact, as Vermeulen points out "The ECtHR has not used the doctrine of the 'essence' of a right in cases relating to article 8, which would act as the ultimate limit of a restriction on article 8. This idea is explained by Judge Matscher's dissenting opinion on the scope of Article 5.1."[1071] Craig stated that the reference to the essence is stringent in EU law, and should be interpreted in accordance with the legal tradition it originates from, namely German law.[1072] Thus far, the Court has not openly struck down a measure based on the essence, and hence its functioning is open to debate. Moreover, as discussed earlier, article 7 paves the way at a minimum to horizontal indirect effects. Finally, article 7 could enjoy greater protection because of the remedies available: legality leading to annulment pursuant to 263 TFEU, and damages liability under article 340 TFEU (additional possibility to the open method coordination),[1073] where the criteria for standing have been broadened.

[1068] Judgment of 16 December 2011 in Satakunnan and Satamedia, C-73/07, EU:C:2008:727; *C-92/09 and C-93/09 - Schecke and Eifert*.
[1069] Judgment of 13 April 2000 in Karlsson and Others, C- 292/97, EU:C:2000:202, para 45.
[1070] The article is not mentioned in the Explanations, but functions as an implicit ground of limitation. Craig (2013).
[1071] Porcedda, Vermeulen and Scheinin (2013), p. 28.
[1072] Craig (2013).
[1073] Ibid.

In *Digital Rights Ireland*, the ECJ strengthened its arguments by relying on the case law of the ECtHR, but performed a test pursuant to article 52.1 of the Charter.[1074] The Court assessed the compatibility of the Data Retention Directive (24/2006/EC) with the rights enshrined in article 7 (and 8) of the Charter based on the following steps:

1) It established whether there was an interference with the rights (§ 35-36);
2) Skipping the legality test, in the clear presence of a legal basis, it assessed whether the interference impinged on the essence (§ 39-40);
3) It analysed to what extent the interference was justified in the light of objectives of general interest recognized by the Union (§ 41- 42);
4) It tackled the proportionality of the interference (§ 45), based on:
    a. The criteria that might limit judicial review: the area concerned; the nature of the right at issue; the nature and seriousness of the interference; the object pursued by the interference (§ 47).
        i. Having established that the interference is very serious (although not as grave as to impinge on the essence, § 48), judicial review should be strict;
    b. The adequacy of the measure to attain the legitimate objectives (§ 46); and
    c. The necessity of the measure to attain the objectives (§ 46, and § 51);
        i. Includes clear and precise rules (§ 54), that is lawfulness;
    d. The limitedness (non-excessiveness) of the measure to what is strictly necessary to attain the objectives (§ 46).

This marks a change with the previous lack of a clear test for permissible limitations.[1075] Before the Charter acquired Treaty-like status, the ECJ either avoided expressing itself on the proportionality of a measure *vis-à-vis* rights recognized in the Charter, as in the so-called 'PNR cases',[1076] or relied entirely on ECHR rights, as in *Schmidberger*.[1077]

This discussion begs the question as to what extent the approach of the CJEU differs from the ECtHR, and whether it affords more protection, taking into account the different powers the two Courts have. This requires a strict comparison of cases that is beyond the

[1074] According to the WP29, the first case featuring an independent elaboration of the test is Schwarz. The report seems to support the idea that the test developed by the CJEU differs from that of the ECtHR. Article 29 Data Protection Working Party (2014), *Opinion 01/2014, WP 211*.
[1075] Craig (2013).
[1076] Judgment of 30 May 2006 in Parliament v. Council, Joined Cases C-317/04 and C-318/04, EU:C:2006:346 (PNR cases).
[1077] Judgment of 12 June 2003 in Schmidberger, C-112/00, EU:C:2003:333.

scope of this chapter. What matters here is that there is a potential mismatch between the two provisions, which needs to be taken into account when appraising the extent to which tackling cybersecurity may interfere with the right to respect for private and family life. Moreover, this discussion is of crucial importance for limitations to the right to personal data protection, the subject of the next chapter, to which I move now.

CHAPTER 7 – THE ATTRIBUTES OF THE RIGHT TO THE PROTECTION OF PERSONAL DATA

This chapter is dedicated to the identification of the attributes and core(s) of the right to the protection of personal data, based on the procedure for extracting the attributes outlined in chapter 5 and used in chapter 6. Accordingly, in section one I review the sources of the right to the protection of personal data relevant in Union law with a view to identifying the attributes. In section two I expound the formulation of the right, particularly in the light of the recently adopted General Data Protection Regulation[1078] (hereafter GDPR) and Directive.[1079]

Section three contains the selection of attributes. The procedure is more experimental than that followed in the previous chapter, since scholarship disagrees on the nature of the independence of the right to the protection of personal data. Yet, the attempt to identify the attributes benefits from the well-established discussion on data protection principles. The attributes will thus result from a mix of principles, relevant case law and authoritative interpretations.

In section four I discuss the regime of permissible limitations of article 8 of the Charter, (as a preliminary step for the application of step four of the methodology identified in chapter 3). I also discuss more broadly the implications of the applicability of the Charter in connection with the implementation of EU law insofar as article 8 is concerned.

1 SOURCES OF THE RIGHT TO THE PROTECTION OF PERSONAL DATA

This section analyses the **sources** of article 8 of the Charter, and partly its scope, as a preliminary step to the identification of the attributes of the right to the protection of personal data. I begin by noting how the sources of article 8 of the Charter are intertwined with article 7 of the Charter, which calls for a reflection on their current import for the identification of

[1078] General Data Protection Regulation (2016/679/EU).
[1079] Directive (EU) 2016/680 on data Protection in Policing.

the attributes. I then analyse in turn four sets of sources: article 8 ECHR, Convention 108 (and the OECD Guidelines), the Treaties and secondary law. In doing so, I reflect on the current import of the sources for article 8 of the Charter.

1.1 THE MULTIPLE SOURCES OF ARTICLE 8 OF THE CHARTER

Article 8 of the Charter reads

> *"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."*

In chapter 1 and 4 I noted that personal data protection, which was initially framed under existing provisions of private life, has subsequently evolved as an independent right in Union law, and perhaps beyond. In fact, according to Zalnieriute,[1080] if one takes a non-orthodox approach to customary international law formation, it may be concluded that "there is a general fundamental right to [so-called] data privacy under customary international law", whose 'international constitutional moment' would go back to legal reactions (*opinio juris*) to the revelations of mass surveillance. In this respect, it becomes particularly important to assess the extent to which the sources of article 8 of the Charter that are also sources of the right to respect for private life matter for the interpretation of an independent right to personal data protection.

As in chapter 4, the figure below shows the interrelated sources of privacy rights. The white sections contain the sources relevant for the right to personal data protection, whereas the grey sections contain sources unique to the right to respect for private and family life.

[1080] Monika Zalnieriute, 'Towards International Data Privacy Cooperation: Strategies and Alternatives' (PhD thesis, European University Institute 2014), p. 114.

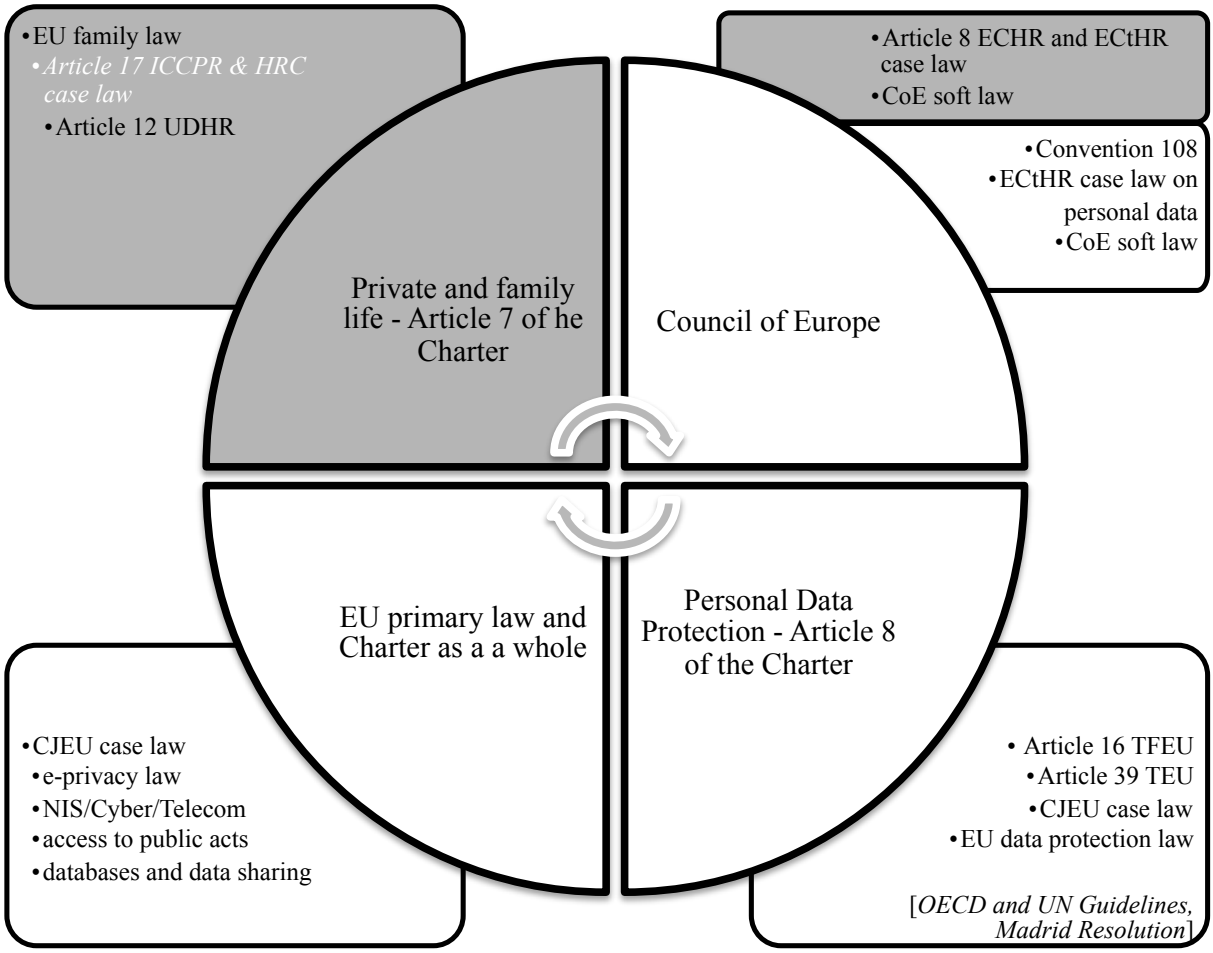


Figure 7 The interrelated sources of privacy rights

The instruments highlighted in this figure include: soft law adopted by consensus, namely the OECD Guidelines,[1081] the United Nations Guidelines[1082] and the Madrid Resolution,[1083] which embody Fair Information Principles (see *infra*, section 1.3) and have played an important role in the 'internationalization' of data protection;[1084] international law treaties which supply guidelines for the interpretation of rights recognized within EU law, i.e. Convention 108[1085] and, possibly, the International Covenant on Civil and Political Rights;[1086]

[1081] OECD Privacy Guidelines.
[1082] General Assembly of the United Nations, 'Resolution 45/95. Guidelines for the regulation of computerized personal data files', (1990).
[1083] International Conference of Data Protection and Privacy Commissioners (2009). Discussed at the International Conference of Data Protection and Privacy Commissioners, held in Madrid on 5 November 2009.
[1084] Such instruments are not *strictu sensu* sources of article 8 of the Charter, however they would become relevant when making the case for the universal application of the attributes of personal data protection.
[1085] Convention 108.
[1086] To the extent that they fall within the purview of article 17 ICCPR in the light of General Comment n. 16, Human Rights Committee cases could also provide guidelines for the understanding of article 8 of the Charter (but the Court has not availed itself of such sources).

the case law of the ECtHR, which has special significance (see *infra* sections 1.2 and 4); CJEU case law on primary and secondary law; and instruments of EU secondary law representing an implementation of the right which determines its current understanding, but which can be overridden at any time by the Courts.

Not all discussed instruments have an import on the Union fundamental right to the protection of personal data. The Explanations to the Charter[1087] list only a subset of the instruments highlighted above, but these still testify to the connection between articles 7 and 8 of the Charter:

> *"This Article has been based on Article 286 of the Treaty…and Directive 95/46/EC…as well as on Article 8 of the ECHR and on the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which has been ratified by all the Member States. Article 286 of the EC Treaty is now replaced by Article 16 of the Treaty on the Functioning of the European Union and Article 39 of the Treaty on European Union. Reference is also made to Regulation (EC) No 45/2001… The above-mentioned Directive and Regulation contain conditions and limitations for the exercise of the right to the protection of personal data."*[1088]

Other than identifying the sources which I will focus on in the remainder, the Explanations could also be read as a compendium of the history of the emergence of the right in the Union (complementary to that in chapter 2, 3.3.2). If article 8 ECHR offered initial 'asylum' to a new need in search of legal protection, it was with the adoption of the Council of Europe Convention 108 (and the related OECD Guidelines, see *infra*, section 1.3) that the idea of 'data privacy', or data protection, surfaced as an internationally relevant concept (and then became global with the adoption of the United Nations Guidelines). Secondary Union law, *in primis* the Data Protection Directive,[1089] explicitly refers to both article 8 ECHR and Convention 108. Such direct connection disappears within the Lisbon Treaty and the GDPR (*infra*, section 1.5); this testifies to the independence of the right, and forces us to reflect on the extent to which the original sources are still relevant to identify the attributes of the right.

In what follows I pursue two objectives. First, I describe each source in a chronological order, with the intention of recalling their importance in the formulation of a right to personal data protection. Second, I reflect on the import of each source for the interpretation of the right enshrined in the Charter, with a view to identifying the attributes. I begin by discussing

[1087] European Parliament, Council and Commission (2002), Explanations to the Charter.
[1088] Ibid.
[1089] Data Protection Directive (95/46/EC).

article 8 ECHR, for which, by means of exception, I address its interpretive import only. This will allow preliminarily defining the material scope of the right to the protection of personal data, and make a stronger case for the need to conceptually distinguish the two privacy rights.

1.2 ARTICLE 8 ECHR, AND ITS IMPORT FOR ARTICLE 8 OF THE CHARTER

What role does article 8 ECHR play for the interpretation of article 8 of the Charter? The question seems to be implicitly answered by much scholarship, which, perhaps subconsciously, conflates personal data protection with the right to respect for private life, particularly in its article 8 ECHR formulation. Yet, in this section I demonstrate that there are good reasons not to perform a casual conflation. I begin with a revision of the approach of the CJEU, and then explain why the two articles should be kept distinct.

1.2.1 THE CONTRADICTORY APPROACH OF THE COURT OF JUSTICE

Recital 10 of Directive 95/46 states that the objective of the instrument is to protect "fundamental rights and freedoms, notably the right to privacy, which is recognized in both article 8 [ECHR] and in the general principles of community law". The recital reflects a state of affairs predating the Charter. However, shortly after the entry into force of the Lisbon Treaty, in *Schecke and Eifert*, the ECJ's Grand Chamber pronounced,

> "*The right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual (see, in particular, European Court of Human Rights, Amann v. Switzerland [GC] ... and Rotaru v. Romania [GC]...) and the limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 of the Convention.*"[1090]

The passage above seems to imply that, similarly to article 7 of the Charter, article 8 has to be read in light of article 8 ECHR. I challenge this argument on two grounds.

The first ground relates to the structure of the Charter, since, differently from article 7 of the Charter, article 8 does not appear in the list of provisions that correspond in full or in part to ECHR rights pursuant to article 52 (3). Rather, I argue that the right to personal data

[1090] *C-92/09 and C-93/09 - Schecke and Eifert*, para 52.

protection could be subsumed under the articles referred to in article 52 (2) of the Charter, whereby

> *"Rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties."*

While the Explanations clarify that article 52 (2) applies to citizens' rights, the combined reading of the Explanations with article 8 and 52 (2), coupled with the formulation of article 16 TFEU (and 39 TEU), seem to imply that the right to the protection of personal data is concerned with article 52 (2) of the Charter. The immediate consequence is that cases concerning the protection of personal data must be interpreted in the light of the Treaties, rather than the ECHR, which would therefore not have primary interpretative value. I discuss the implications of this argument for secondary law in section 1.5.

The second ground is that the CJEU has not been consistent in its approach ever since it recognized the existence of an autonomous right to personal data protection with the case *Promusicae.*[1091] The Court seems to take three approaches: merging the right to respect for private life with the protection of personal data; distinguishing the two rights, but instead of carrying out distinct analyses, mixing considerations on both (sometimes to the effect of confusing them); and analysing the cases under the sole lens of personal data protection.

First, the ECJ analysed personal data protection under the lens of article 8 ECHR, as in *Österreichischer Rundfunk and Others*[1092]*,* and private life,[1093] such as *Lindqvist,*[1094] in the *Schecke and Eifert*[1095] case, and even *the Google Spain and Google* case,[1096] where the ECJ refers to the "right to privacy with respect to the processing of personal data" (§ 58, 66 and 74) as formulated in the Data Protection Directive. As anticipated in chapters 2 and 6, such an approach, which may be tied to the Court's respect for the formulations contained in the still legally binding Data Protection Directive, may change soon, since the GDPR refers solely to article 8 of the Charter and article 16.1 TFEU (see *infra*, section 1.5).

[1091] Judgment of 29 January 2008 in Promusicae, C-275/06, EU:C:2008:54.
[1092] *Joined cases C-465/00, C-138/01 and C-139/01 - Österreichischer Rundfunk*.
[1093] Gloria Gonzàles Fuster, 'Balancing Intellectual Property against Data Protection: a New Right's Wavering Weight' in A. Cerrillo i Martínez and others (eds), *Challenges and Opportunities of Online Entertainment Proceedings of the 8th International Conference on Internet, Law & Politics Universitat Oberta de Catalunya* (UOC-Huygens Editorial 2012).
[1094] Judgment of 6 November 2003 in Bodil Lindqvist, C-101/01, EU:C:2003:596.
[1095] *C-92/09 and C-93/09 - Schecke and Eifert*.
[1096] *C-131/12 - Google Spain and Google*.

Second, *Digital Rights Ireland* offers an example of cases where the Court distinguishes between the interference caused by data retention to articles 7 and 8 of the Charter,[1097] but mixes considerations of both, with contradictory outcomes. For instance, in paragraph 33 the Court states "to establish the existence of an interference *with the fundamental right to privacy*, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way" (emphasis mine). That passage is taken, in turn, from ground 75 of the abovementioned *Österreichischer Rundfunk and Others*, and is misquoted, in that the original referred to 'private life' instead of privacy,[1098] interpreted in the light of article 8 ECHR. The Court seems to interpret article 8 of the Charter (to which the adjective 'sensitive' should relate) in the light of article 7, read in turn in the light of article 8 ECHR. This passage is further taken up in *Schrems.*[1099] A similarly confusing interpretation, where elements of the right to the protection of personal data are used to characterize an infringement of private life, is found, *inter alia,*[1100] in *YS and others*[1101] (discussed in chapter 6, section 3.3.1). Further on in *Digital Rights Ireland*, the Court states that "the protection of personal data resulting from the explicit obligation laid down in article 8(1) of the Charter is especially important for the right to respect for private life enshrined in article 7 of the Charter".[1102] In this case, the infringement of the first may be sufficient to determine the infringement of the second (and not vice versa). In other words, the Court seems to say that, if there is a violation of article 8, then there is a violation of article 7.

[1097] *Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*, para 29. It interestingly quotes Schecke and Eifert (para 47).

[1098] Elsewhere, the Court referred to privacy as relating to article 8 of the Charter: "In view of the importance…of protecting privacy, emphasised in the case-law of the Court (see Rijkeboer, § 47 and the case-law cited) and enshrined in Article 8 of the Charter, the fees which may be levied under Article 12(a) of the directive may not be fixed at a level likely to constitute an obstacle to the exercise of the right of access guaranteed by that provision." Judgment of 12 December 2013 in X, C-486/12, EU:C:2013:836, para 29.

[1099] *C-362/14 - Schrems*, para 87.

[1100] For instance, "the significance of the data subject's rights arising from Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter')." And "In this regard, it must be noted that Article 8(1) of the Charter states that '[e]veryone has the right to the protection of personal data concerning him or her'. That fundamental right is closely connected with the right to respect for private life expressed in Article 7 of the Charter". Judgment of 24 November 2011 in ASNEF and FECEDM, joined cases C-468/10 and C-469/10, EU:C:2011:777, paras 40 and 41. Moreover, "…according to settled case-law, the protection of the fundamental right to private life guaranteed under Article 7 of the Charter of Fundamental Rights of the European Union ('the Charter') requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary". Judgment of 11 December 2014 in Ryneš, C-212/13, EU:C:2014:2428, para 28.

[1101] *Joined cases C-141/12 and C-372/12 - YS and others*, para 44. "As regards those rights of the data subject, referred to in Directive 95/46, it must be noted that the protection of the fundamental right to respect for private life means, *inter alia*, that that person may be certain that the personal data concerning him are correct and that they are processed in a lawful manner".

[1102] *Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*, para 53.

Third, the Court relied solely on article 8 of the Charter in *Deutsche Telekom,*[1103] *Scarlet Extended*[1104] and *Sabam.*[1105]

In any event, despite its contradictory approach, the ECJ has not openly reinstated that (limitations to) article 8 of the Charter should be read in the light of article 8 ECHR. This begs the question of the implications of forgoing a strict equation between article 8 ECHR and 8 of the Charter.

1.2.2 GOING BEYOND THE PROTECTION AFFORDED BY ARTICLE 8 ECHR

Abandoning a strict equation between article 8 ECHR and article 8 of the Charter is fundamental because the ECtHR interprets the protection of personal data restrictively. Kranenborg noted that, in interpreting cases concerning personal data, the ECtHR "excludes from the scope of the protection of privacy under Article 8 ECHR the processing (…) of personal data: i) which is (*sic*) not private in itself; ii) which are not systematically stored with a focus on the data subject; and iii) if the data subject could reasonably expect the processing (disclosure)."[1106] A case in point is *Pierre Herbeq and the association "Ligue des droits de l'homme".*[1107] In the case (which was discussed prior to the adoption of Directive 95/46/EC), the applicant alleged that the absence of a law applying to video surveillance that does not record the images filmed breached his rights under article 8 ECHR, in that they could lead to self-censoring one's behaviour. The ECtHR noted that, in the absence of recording, the activities of the surveillance camera simply observed "public behaviour" as any passers-by would. As a result, it ruled that the complaint of the applicant was manifestly ill founded. Yet, so long as an identified or identifiable individual is concerned, EU law would define this as processing of personal data, which would be unlawful in the absence of a legal basis or other legitimate ground for processing, such as consent[1108] (see *infra*, section 2.2).

Even if, so far, the ECJ has not clarified once and for all the import of article 8 ECHR, it has already taken a different approach on the three points mentioned by Kranenborg. In the

[1103] Judgment of 5 May 2011 in Deutsche Telekom, C-543/09, EU:C:2011:279.
[1104] *C-70/10 - Scarlet Extended.*
[1105] *C-360/10 - Sabam.*
[1106] Kranenborg (2008), p. 1093.
[1107] Herbecq and the Association "Ligue Des Droits De L'homme" v. Belgium, n. 32200/96 and 32201/96, CE:ECHR:1998:0114DEC003220096 (European Court of Human Rights).
[1108] Article 29 Data Protection Working Party, *Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance* (11750/02/EN WP 89, 2004).

Bavarian Lager Ltd. case, decided by the ECJ in the Grand Chamber composition only a couple of months before *Schecke and Eifert*, the Court pronounced

> *"The General Court limits the application of the exception under Article 4(1)(b) of that regulation to situations in which privacy or the integrity of the individual would be infringed for the purposes of Article 8 of the ECHR and the case-law of the European Court of Human Rights, without taking into account the legislation of the Union concerning the protection of personal data, particularly Regulation No 45/2001. (...) Article 1(1) of Regulation No 45/2001...does not allow cases of processing of personal data to be separated into two categories, namely a category in which that treatment is examined solely on the basis of Article 8 of the ECHR and the case-law of the European Court of Human Rights relating to that article and another category in which that processing is subject to the provisions of Regulation No 45/2001."*[1109]

In particular, article 8 of the Charter protects personal data regardless of a connection with private life, and hence "it is not necessary in order to find such a right [of deletion of one's data] that the…information in question…causes prejudice to the data subject."[1110] *A contrario*, the sole processing of personal data "constitutes an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter."[1111]

Hence, for all its incoherence, the ECJ has gone further than the ECtHR in safeguarding personal data, in line with the understanding of personal data enshrined in Union secondary law (see *infra*, section 1.5). Indeed, secondary law, owing *inter alia* to its level of detail, is more protective of the right than that which the interpretation of the ECtHR could offer. In other words, treating personal data protection as an independent right has the advantage of providing greater protection than that offered, in the past and prospectively, by the ECHR. Lynskey[1112] notes that the differentiation, which benefits from the narrow construction of exceptions to restrictions of fundamental rights pursued by the ECJ, is reinforced by the GDPR, which identifies more rights for the data subject (see *infra*, section 2.2.2). Another advantage consists in reaffirming the independence of Union law, whose application could be imperilled by the restrictive approach of the ECtHR, an outcome abhorred by the Court, which in its opinion on the accession to the ECHR pronounced "any action by the bodies given decision-making powers by the ECHR, as provided for in the agreement envisaged,

[1109] *C-28/08 P - Bavarian Lager Ltd.*, paras 58 and 61.
[1110] *C-131/12 - Google Spain and Google*, para 96.
[1111] *Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*, para 36.
[1112] Lynskey (2015).

must not have the effect of binding the EU and its institutions, in the exercise of their internal powers, to a particular interpretation of the rules of EU law."[1113] As a result, the case law of the ECtHR will not be relied upon in the identification of the attributes.

The foregoing does not imply the irrelevance *tout court* of article 8 ECHR, which, as noted several times, is an instrument of special significance within the Union legal order. The reflections of Kranenborg prove, once more, useful in this respect. Kranenborg envisages three situations determined by the difference in scope of 'privacy' (private life) and data protection: "Situation 1: disclosure of personal data is outside the scope of privacy protection and within the scope of data protection;[1114] Situation 2: disclosure of personal data is within the scope of privacy protection and within the scope of data protection; Situation 3: disclosure of personal data is within the scope of privacy protection and (within the data protection rules) within the special regime for the protection of sensitive data."[1115] In situation 1, the ECtHR would not supply guidelines for the interpretation of article 8 of the Charter; in situations number 2 and 3, the relevant case law of the Strasbourg Court would supply guidelines of special significance, which indeed the ECJ has used 'by analogy'. Such cases concern the interpretation of the ECHR in the light of Convention 108, to which I turn next.

1.3 CONVENTION 108

Convention 108[1116] and its additional protocol[1117] was the first international legal elaboration of data protection, adopted to compensate for the limitedness of the ECHR, written before the ubiquity of computers. In this respect, it is the *lex specialis* laying down rules on the processing of personal data relied upon by the ECtHR (since *Z. v. Finland* and *Rotaru v. Romania*) in article 8 cases concerning personal information.

While the Explanations to the Charter do not make reference to the OECD Privacy Guidelines (also recently revised[1118]), the latter were very influential in the parallel drafting of

[1113] *Opinion of the Court 2/13*, para 184.
[1114] Advocate General Kokott seems to support this view when she stated that the right to personal data protection captures dimensions otherwise not protected by private life. Kokott and Sobotta (2013).
[1115] For him, "The interest of the data subject increases gradually." Kranenborg (2008), 1094.
[1116] Convention 108 (footnote n. 1085).
[1117] 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, Council of Europe, CETS n.181, 8 November 2001.
[1118] OECD Privacy Guidelines. (1081).

Convention 108, and must therefore be mentioned in order to understand it.[1119] Within their different remit, both the Guidelines and the Convention provided an elaboration of the so-called "fair information principles" [1120] (hereafter FIPs), i.e. the rules of thumb for processing personal data, thus addressing the obstacles for the free flow of personal data and paving the way to the formulation of a right to data protection. The FIPs incorporated in the original version of the OECD Guidelines were: collection limitation; data quality; purpose specification; use limitation; security safeguards; openness; individual participation; and accountability.

Convention 108 includes most of the FIPs. Article 5 on the quality of the data encompasses the principles of collection limitation, data quality, purpose specification, and use limitation. Article 7 on data security embodies the security safeguards principle. Article 8 on additional safeguards for the data subject encompasses the principles of individual participation and openness. While article 10 on sanctions and remedies lays down that misdeeds will be punished, there is no explicit provision on accountability. Moreover, Convention 108 created the special categories of personal data that cannot be processed automatically unless domestic law provides appropriate safeguards (article 6). Such data are those revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life and data relating to criminal convictions. Such innovation has become a staple of Union legislation, and creates a functional *trait d'union* with other rights, including but not limited to the prohibition of discrimination and the right to respect for private life. The table below shows the correspondence between the fair information principles enshrined in the OECD Guidelines, and those enshrined in Convention 108.

[1119] Explanatory Memorandum of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe. See in particular the section "Co-operation with OECD and the EEC". It should be recalled that the OECD has since then acted as a forum of discussion for a number of issues, such as the cross-border enforcement of privacy laws and the demand for standards to ensure the security of personal data as part of a wider cyber-security strategy, e.g. Organization for Economic Cooperation and Development (OECD) (2002). Thus, it acted as an arena to confront opposing views, particularly those of the US and the EU, and to understand them. In the opinion of Bennett and Raab, the OECD Guidelines were an attempt to justify self-regulatory approaches. Bennett and Raab (2006).

[1120] See, among others, Bennett and Raab (2006); Gellman (2012).

Principles/ Instrument	Purpose specification	Use limitation	Collection limitation	Openness	Individual participation	Data quality	Accountability	Security	New: Independent control
OECD Guidelines	X	X	X	X	X	X	X	X	
Convention 108	X	X	X	X	X	X		X	X

Table 14 Fair information principles in the OECD Guidelines and Convention 108

Convention 108 has played and continues to play an important role in EU law. To begin with, it was a harmonizing factor in the field of data protection law for the Member States of the then European Communities.[1121] As important, Convention 108 was very influential in the adoption of the Data Protection Directive, which reproduces its structure and draws heavily from its content.[1122] Indeed, recital 11 of the Data Protection Directive states that the "principles…contained in this Directive, give substance to and amplify those contained in [Convention 108]," thus expressing a *renvoi* or connection clause.[1123] Hence, Convention 108 acts as the *trait d'union* between Strasbourg and Brussels on data protection matters. The formulation of FIPs in Convention 108 forms the bedrock of Union secondary data protection law, which thus represents the best heir of the Council of Europe's legacy. In this respect, Convention 108 is an indirect, yet particularly important source of article 8 of the Charter. Not only does the Data Protection Directive represent a specification of the right (see *infra* section 1.5), but it also informs the very formulation of the right (see *infra*, section 2).

In 1999 Convention 108 was amended to enable the then European Communities to accede to it.[1124] The Protocol to Convention 108 enabling the Union to accede includes

[1121] Here I should recall that, in this thesis, I look at the obligations arising from these instruments upon Member States and institutions of the European Union *qua* components of the Union. The consequences produced by the interaction of rules of national law that fall outside the remit of EU law, and provisions of international instruments, are beyond the scope of this research.
[1122] European Union Network of Independent Experts on Fundamental Rights (2006).
[1123] On the topic of connection clauses, see Cremona (2016), 'A Triple Braid: Interactions between International Law, EU Law and Private Law'; Christiaan Timmermans, 'The Specificity of Private Law in EU External Relations: The Area of Freedom, Security, and Justice' in Marise Cremona and Hans-W Micklitz (eds), *Private Law in the External Relations of the EU* (Oxford University Press 2016).
[1124] Amendments to Convention 108 approved by the Committee of Ministers, in Strasbourg, on 15 June 1999.

Regional Economic Integration Organization clauses disciplining voting rights (article 2 (3)), but not a disconnection clause.[1125] One of the reasons may be the uncontroversial role of the two data protection Directives already in force at the time in the Union, also signalled by the fact the European Communities acquired exclusive voting rights, equal to the number of their Member States, on matters over which Member States had transferred their competence. As important, there could be a division of labour between Union law and Convention 108. In the words of the Explanatory memorandum on the amending protocol "Accession by the Communities reflects the European Union's wish to develop co-operation with the Council of Europe and help create a stronger international forum on data protection, particularly *vis-à-vis* third countries". Thus far, no accession has followed, but the explicit connection clauses to it may lead to it producing binding effects in Union law, were the CJEU made to express itself on it.[1126] In the next section, I reason on the import of Convention 108 also in relation to its potential applicability in Union law.

1.3.1 Revised Convention 108: import on Union law and relevance of for the identification of the attributes

Convention 108 is currently undergoing a process of revision,[1127] and the Union is taking part in the negotiations. The import on Union law of Convention 108 will depend on whether the Union signs (and ratifies) the revised text.

Should the Union sign and ratify the revised Convention, it would become a mixed agreement,[1128] and as such subject to the provisions of article 3 (5) TEU and 216 TFEU (2), and the copious, albeit contradictory,[1129] case law on the subject matter. Hence, Convention 108 would be binding upon the Union and its member states, forming an integral part of EU law.[1130] While the new Convention 108 would not have primacy over primary law, including

[1125] Marise Cremona, 'Who Can Make Treaties? The European Union' in Duncan Hollis (ed), *The Oxford Guide to Treaties* (Oxford University Press 2012); Jean-Claude Juncker, *Council of Europe – European Union: a sole Ambition for the European Continent* (Report to the Attention of Heads of State or Government of the Member States of Council of Europe, 2006).
[1126] Cremona (2016), 'A Triple Braid: Interactions between International Law, EU Law and Private Law'.
[1127] Ongoing since 2011: http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp.
[1128] For a discussion of the impact of mixed agreements, see Cremona (2012), 'Who Can Make Treaties? The European Union'.
[1129] Craig and de Búrca (2015).
[1130] Following the Case of *Haegenam*, C-181/73, discussed in Cremona (2012), 'Who Can Make Treaties? The European Union'; Craig and de Búrca (2015).

general principles and fundamental rights,[1131] it would enjoy greater force than secondary law, including the GDPR and the Directive in the AFSJ, which should be interpreted in a manner consistent with it.[1132] To be sure, as Cremona[1133] noted, if the EU became a party it would be for the CJEU to interpret the provisions of Convention 108 to determine their legal effect, including their capability to produce direct effect, and the need for consistency between the two texts. The most recent version of the text (dating May 2016), like the original Convention, does not contain a disconnection clause.

How likely is the EU to sign Convention 108? On the one hand, the simultaneous and intertwined revisions of Union law and Convention 108 could be an indication of the Union's willingness to accede to the instrument. The most recent version of the text includes a number of reservations of the European Union "in order to ensure consistency with the European Union reform", and the text is striking for its resemblance to the changes contained in the GDPR. On the other hand, the absence in the GDPR of clear connection clauses, as the Data Protection Directive has, may signify the Union's unwillingness to sign the Convention.

In the GDPR, Convention 108 is only mentioned in recital 105 of the GDPR, as an important factor in assessing the adequacy of the data protection legislation of third countries and organizations, with a view to allowing the transfer of personal data: "third country's accession to [Convention 108] and its Additional Protocol should be taken into account." In this vein, the repeal of the Data Protection Directive could be seen as signalling the intention to take some distance from the old Convention 108, which would no longer have a direct import on the interpretation of article 8 of the Charter. However, Convention 108 would still have a role to play for the interpretation of the attributes, particularly due to the active role played by the Union in the negotiations of the revised text. Such an active role, which may be in line with the spirit of the original envisaged accession of reflecting the "Union's wish to help create a stronger international forum on data protection, particularly vis-à-vis third countries", could be an example of contributing to the double external relations objective discussed by Cremona, i.e. of taking part in international rule-making whilst exporting its rules.[1134] Recital 105 of the GDPR could reinforce this reading: Convention 108 may

[1131] After Kadi, as discussed in Cremona (2012), 'Who Can Make Treaties? The European Union'; Craig and de Búrca (2015).
[1132] Following the case of Commission v. Germany, C-61/94, discussed in Cremona (2012), 'Who Can Make Treaties? The European Union'; Rosas and Armati (2010).
[1133] Cremona (2012), 'Who Can Make Treaties? The European Union'.
[1134] Cremona (2011), 'Values in EU Foreign Policy'.

represent the minimum standards to consider the legislation of third countries adequate,[1135] whereas Union law would go further and ensure greater protection.

The meaningful conclusion is that the revised Convention 108 is relevant for the identification of the attributes irrespective of the role played for the interpretation of the right, because the new text embodies what are considered, for the time being, the minimum standards for the protection of personal data in Union law. This marks a difference with the role played by the ECHR, as discussed in the previous section, and as summarized in the table below.

Treaty	**ECHR**	**Convention 108 - old**	**Convention 108 -new**
Interpretation	Special significance	Supplies guidelines	Supply guidelines OR interpretation that conforms
Attributes	no	no	Yes

Table 15 ECHR v. Convention 108 on the interpretation of article 8 of the Charter and its attributes

Before moving to the sources of article 8 of the Charter in primary law, I should recall that Convention 108 remains a benchmark in areas that fall outside the scope of EU law, and hence of the Charter (see *infra*, section 4).

1.4 SOURCES OF ARTICLE 8 OF THE CHARTER IN THE TREATIES AND EU LAW

Article 286 TEC, replaced by article 16 TFEU and 39 TEU, is the first source mentioned by the Explanations. The two Treaty provisions effect two operations. First, they sanction the status and independence of the right; secondly, they delegate to secondary law to provide additional meaning to the right.

As for the first, in keeping with article 8 of the Charter, article 16 TFEU does not hinge on economic motivations, but rather frames the protection of one's personal data as a right

[1135] On the notion of adequacy, the ECJ stated "The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter." *C-362/14 - Schrems*, para 71.

(see also chapter 1)[1136]. Moreover, article 16 TFEU is formulated in a way capable of producing direct effects.[1137] The right is not conceived of as absolute, and in fact article 16 TFEU has to be read in combination with other Treaty elements.

On the one hand, article 16 TFEU should be read together with Declaration n° 20 to the Treaty, which clarifies that rules adopted on the basis of article 16 TFEU shall provide for specific derogations when directly affecting national security, which is outside of the scope of EU law (see *supra*, section 1.3), and Declaration n° 21 to the Treaty, encouraging the adoption of specific rules on data processing in the fields of judicial cooperation in criminal matters and police cooperation.[1138] This is the recently adopted Directive on processing in the AFSJ, substituting the much-criticized[1139] Council Framework Decision 977/2008/JHA,[1140] and addressing what has long been a legal grey area.[1141] It will apply to the prevention, investigation, detection and prosecution of criminal offences, but not to national security, which is the sole responsibility of Member States (article 72 TFEU).[1142]

On the other hand, Article 16 must be read in combination with another source of the fundamental right to personal data protection, article 39 TEU, which lays down special rules for the processing of data in the common foreign and security policy (hereafter CFSP), where

[1136] To this effect, see also Lynskey (2015).
[1137] 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?' (2009) 46 Common Market Law Review 1485-1525.
[1138] Ibid.
[1139] According to Vermeulen, the instrument has several limitations. First, its scope of application includes cross-border exchange of personal data within the EU, but not domestic processing operations in the member states, which creates practical hurdles. Second, the combined reading of articles 13 and 26 on exchanges of personal data outside the EU betrays the idea, expressed in recital 23, whereby transfers can take place solely if the recipient ensures an adequate level of protection. Third, there is no mechanism to distinguish between data having different degrees of accuracy and reliability. Finally, the Decision does not replace the various sector-specific legislative instruments, thus affecting the exercise of the data subject's rights. Porcedda, Vermeulen and Scheinin (2013); Frank Dumortier and others, 'La Protection des Données dans l'Espace Européen de Liberté, de Sécurité et de Justice' 166 Journal de Droit Européen 23; European Commission, *A Comprehensive Approach on Personal Data Protection in the European Union* ((Communication) COM (2010) 609 final, 2010).
[1140] 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.
[1141] The original data protection strategy encompassed a draft resolution extending the application of the general directive to those areas falling outside the scope of Community law, which was only adopted as Council Framework Decision 2008/977/JHA. European Commission, *Directive Concerning The Protection of Individuals in Relation to the Processing of Personal Data, Recommendation for a Council Decision on the Opening of Negotiations With a View to the Accession of the European Communities to the Council of Europe Convention for the Protection of Individuals With Regard to the Automatic Processing of Personal Data, Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security* ((Communication) COM (90) 314 final, 1990).
[1142] This is an area subject to the 'pre-emption' clause, whereby member states can "exercise their competence to the extent that the Union has not exercised its competence" (article 2 TFEU, paragraph 2), which will necessarily affect the exercise of the exclusive competence of Member States in the maintenance of law and order and the safeguarding of internal security (article 72 TFEU).

the Charter applies, although *vis-à-vis* a limited jurisdiction of the Court.[1143] No rules have been adopted yet pursuant to article 39 TEU.

The distinction between rules adopted pursuant to articles 16 TFEU and 39 TEU is not a clear one, and becomes blurred in the so-called external area of the AFSJ.[1144] The external area of the AFSJ is the overlapping policy sector of the AFSJ and CFSP (and CSDP) that resulted from the internationalization of domestic security threats,[1145] and which has acquired special prominence due to the increase in international intelligence-led policing, and the tendency to regulate data exchanges by means of international agreements. This is an area likely to play increasing importance in relation to cybersecurity.[1146] Even if the Lisbon Treaty does not contain clear rules to select the appropriate legal basis[1147] for data processing activities in the external area of the AFSJ, fundamental rights obligations apply in full irrespective of the legal basis chosen (see *Parliament v. Council* in the context of restrictive measures[1148] and CFSP[1149]). Furthermore, it should also be noted that, pursuant to article 21(2)(a) TEU, foreign policy and international cooperation action is informed by the safeguarding of EU values (which include human dignity, freedom and the respect for human rights, listed in article 2 TEU), fundamental interests, security (which is also one of the objectives of the EU, pursuant to article 3 TEU), interdependence and integrity. External action shall be guided by the principles that inspired the creation of the EU, which include the universality and indivisibility of human rights and fundamental freedoms, as well as the respect for the principles of the United Nations and international law.[1150]

As for the second operation, both article 16 TFEU and 39 TEU lay down a positive obligation for the legislator to adopt new rules pertaining to the "protection of individuals with regard to the processing of personal data" and the free movement of such data, by EU

[1143] Christophe Hillion, 'Decentralised Integration? Fundamental Rights Protection in the EU Common Foreign and Security Policy' (2016) 1 European Papers - A Journal on Law and Integration; Opinion of Advocate General Bot of 30 January 2014 in European Parliament v. Council, C-658/11, EU:C:2014:41, para 119. See also Herlin-Karnell (2013), 'EU Values and the Shaping of the International Legal Context'. On the nature of the CFSP within the treaties, see Cremona (2012).

[1144] *Council, Draft Internal Security Strategy for the European Union: Towards a European Security Model, 5842/2/10* (2010), 16.

[1145] See, among others, Marise Cremona, Joerg Monar and Sara Poli (eds), *The External Dimension of the European Union's Area of Freedom, Security and Justice* (Peter Lang 2011).

[1146] See, to this effect, European Commission and High Representative of the European Union for Foreign Affairs and Security Policy (2016), *JOIN (2016) 18 final*.

[1147] For a test to adjudicate on the appropriate legal basis, see Judgment of 19 July 2012 in Parliament v. Council, C-130/10, EU:C:2012:472, paras 42-25. On the relevance of choosing the appropriate legal basis, see Cremona (2012), 'Who Can Make Treaties? The European Union'.

[1148] *C-130/10 - Parliament v. Council*, paras 83-84.

[1149] Judgment of 14 June 2016 in Parliament v. Council, C-263/14, EU:C:2016:435, para 47.

[1150] On this point, see also Cremona (2011), 'Values in EU Foreign Policy'.

institutions, bodies, offices and agencies, and by the Member States within the scope of EU law. It is to secondary law that I move onto now.

1.5 THE ROLE OF UNION SECONDARY LAW

The Explanations refer to the Data Protection Directive and Regulation 45/2001[1151] as sources of inspiration of article 8 of the Charter. The former is the *lex generalis* disciplining most processing of personal data and "designed to ensure, in the Member States, observance of the right to protection of personal data."[1152] The Directive incorporated the principles elaborated in Convention 108 (and the OECD Guidelines) and expanded them further. As highlighted above, it also embraced the idea of a reinforced regime of protection for special categories of data.

Principles / Instrument	**Purpose specification**	**Use limitation**	**Collection limitation**	**Openness**	**Individual participation**	**Data quality**	**Accountability**	**Security**	**New: Independent control**	**New: lawfulness**
OECD Guidelines	X	X	X	X	X	X	X	X		
Convention 108	X	X	X	X	X	X		X	X	
Data Protection Directive	X	X	X	X	X	X		X	X	X

Table 16 Distribution of FIPs in the OECD Guidelines, Convention 108 and Data Protection Directive

[1151] 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 L 8.
[1152] *C-543/09 - Deutsche Telekom*, para 50.

Regulation 45/2001 extends the level of protection afforded by the Data Protection Directive to the bodies and institutions of the Union. In fact, in *YS*, the Court stated that "Directive 95/46 and Regulation No 45/2001 have, in essence, the same objectives."[1153] The Regulation establishes "a 'fully-fledged system' of protection of personal data… to ensure throughout the Community 'consistent and homogeneous application of the rules for the protection of individuals' fundamental rights and freedoms with regard to the processing of personal data."[1154] It sets up the European Data Protection Supervisor (hereafter EDPS), tasked with supervising, consulting and advising the Union institutions, bodies and agencies over the application of the Regulation. In the words of the Explanations, both instruments "contain conditions and limitations for the exercise of the right to the protection of personal data".

References to Union secondary law beg the question of the role played by such secondary law in the interpretation of the right. As discussed earlier in section 1.2.1, the wording of the Explanations, whereby the Directive and Regulation "contain conditions and limitations for the exercise of the right to the protection of personal data", recalls that of article 52(2) of the Charter.[1155]

Reading article 8 of the Charter through the lens of article 52(2) means, as suggested by Craig,[1156] that the CJEU should take into sufficient account secondary law, whenever this has extensively refined the purview of a right whose legal basis is found in the Treaty. This could be supported by what the ECJ said, among others, in *Google Spain and Google*, whereby the requirements of article 8(2) and 8(3) of the Charter "are implemented *inter alia* by Articles 6, 7, 12, 14 and 28 of Directive 95/46".[1157]

Accordingly, secondary Union law pursuant to both articles 8 of the Charter and 16 TFEU should be taken into account when interpreting the scope of exercise of the right (for limitations in particular, see *infra*, section 4). Hence, secondary law will be relied upon to detail the formulation of the right and the attributes.

[1153] *Joined cases C-141/12 and C-372/12 - YS and others*, para 46.
[1154] *C-28/08 P - Bavarian Lager Ltd.*, para 51.
[1155] Art 52 (2) reads "Rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties."
[1156] Otherwise article 52.2 would be in tension with the idea that the provisions of the Charter enjoy the same legal status as the Treaties, as constitutional provisions could be limited by secondary legislation, whenever the Treaty provisions are formulated in generic terms; it would also conflict with the idea that fundamental rights are used as instruments to challenge the validity of EU law. Craig (2013).
[1157] *C-131/12 - Google Spain and Google*, para 69. This reconciles the opposition of Orla Lynskey to seeing the Directive as an interpretation of the right, due to the prevalence in it of the market objective. Lynskey (2015).

As discussed in section 1.2, this also means that, with a view to safeguarding the system of protection of personal data offered within the Union, the case law of the ECtHR on article 8 ECHR (especially those referring to Convention 108, see *supra,* section 1.3) should hold special significance in the interpretation of the scope and meaning of the fundamental right to the protection of personal data, whenever the ECtHR touches upon the issue (as discussed *supra*, section 1.2.2), but not supersede Union law in case of conflict, owing to the wider protection that can and should be granted under Union law.

As for the specific instruments mentioned in the Charter, the Data Protection Directive will be soon replaced by the GDPR, which will enter into force in May 2018 and will serve as the main reference to interpret the meaning and scope of the right to the protection of personal data (or Directive 2016/680 in the AFSJ, see *supra*, section 1.4). Such intervention was justified[1158] by the impact on data protection of the combination of advances in technological applications[1159] and the changing nature of international data flows, as well as the divergence of approaches in the member states.[1160]

The GDPR responds to the positive obligations set out in article 16.2 TFEU in a way that seems to be clearly privileging the protection, rather than the free flow, of the data.[1161] It also implies the revision of Regulation 45/2001/EC and Directive 58/2002/EC,[1162] which acts as a *lex specialis* for data processing in the telecommunications sector.[1163]

[1158] Article 29 Data Protection Working Party and 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, 2009).

[1159] See, for instance, Viviane Reding, *The Review of the EU Data Protection Framework, SPEECH/11/183* (2011); Giovanni Buttarelli, 'Latest Developments in Data Protection' (Presentation at the meeting of the Heads of Agencies, Stockholm, 19 October 2012).

[1160] See, in this respect, the Judgment of 7 November 2013 in IPI, C-473/12, EU:C:2013:715, para 31. "…the Court has also found that the provisions of Directive 95/46 are necessarily relatively general...and that the directive includes rules with a degree of flexibility and, in many instances, leaves to the Member States the task of deciding the details or choosing between options".

[1161] Bert-Jaap Koops noted that such an approach may fail to win the ear of data controllers, thus undermining the protection of personal data. Bert-Jaap Koops, 'The Trouble with European data Protection Law' (2014) 4 International Data Privacy Law 205-261.

[1162] E-Privacy Directive (2002/58/EC).

[1163] "The Directive on privacy and electronic communications clarifies and supplements Directive 95/46 in the electronic communications sector." *C-543/09 - Deutsche Telekom*, para 50.

2 FORMULATION OF ARTICLE 8 OF THE CHARTER, AND SCOPE

Owing to its statutory origin,[1164] Article 8 is particularly detailed in comparison to other articles in the Charter. In what follows, I expound the content of the right which, following from the discussion in section 1, is based on primary and secondary law as interpreted by the CJEU, and takes into due account the current draft (May 2016) of Convention 108. Such an operation is preliminary to the identification of the attributes (see *infra*, section 3).

2.1 PARAGRAPH ONE: THE *LEX GENERALIS*

Article 8.1 reads

> *"Everyone has the right to the protection of personal data concerning him or her."*

Article 8.1 acts as a *lex generalis*: it enunciates the general rule whereby individuals enjoy the right to having their personal data protected. The formulation has been copied *verbatim* in the first paragraph of article 16 TFEU. Here I discuss the notion of personal data and of protection.

2.1.1 THE NOTION OF PERSONAL DATA

To begin with, the right provides an entitlement to the protection of one's own data (with the exceptions specified by secondary law). The notion of personal data, enshrined in article 2(a) of Directive 95/46/EC, is composed of four cumulative elements,[1165] which have been maintained in the GDPR (article 4.1). First, personal data refers to 'information,' regardless of its degree of sensitivity, format (paper, electronic, audio) and truthfulness.[1166]

Second, such information is 'personal' in that it must be either (directly or indirectly) about an individual, or used for the purpose of affecting an individual; or resulting in affecting an individual. Know-how is excluded from the notion of personal data. Deceased

[1164] Bygrave (2014).
[1165] Article 29 Data Protection Working Party (2007), *Opinion 4/2007, WP 136*.
[1166] According to Lynskey (2015), this interpretation could be challenged by the decision of the ECJ in *YS*, where it pronounced that "legal analysis does not constitute personal data, even if it may contain personal data (§ 39)". This may be more of an effective remedy issue then a personal data one.

individuals do not enjoy the protection of the GDPR (recital 27), but Member States can determine rules for data concerning them.

Third, the person must be 'identified or identifiable' (through so-called 'identifiers'), i.e. it must be possible to distinguish such person from all other members of the group, through means that are likely to be used (recital 26 of Directive 95/46 and 26 of the GDPR). The means are conceived of in evolutionary terms: a dynamic test should be applied to technological developments, in order to assess the potential capability of a technology to 'identify' individuals.[1167] In the attempt to bridge a 17-year technological divide with the Data Protection Directive, article 4(1) of the GDPR broadens the notion of identifiers, and includes online identifiers,[1168] location data, and factors relating to mental identity.

Fourth, the individual must be a "natural person" (data subject), that is, a human living being, regardless of residence and nationality. Unlike the Directive, the GDPR does not protect legal persons' data (article 1(2) and recital 14). This is unfortunate, "since problems concerning the processing… can affect both legal and natural persons,"[1169] with the exception of physical, physiological and mental data. Currently the personal data of legal persons are protected "in so far as the official title of the legal person identifies one or more natural persons"[1170] if they fall under the restricted cases of the e-Privacy Directive, which explicitly mentions the legitimate interest of the subscribers who are legal persons, as regards articles 12 and 13 on unsolicited communications (in this case, the case law of the ECtHR which recognises the protection of a sphere of privacy to legal persons could become more protective *vis-à-vis* the GDPR).[1171] The Court had noted, however, that "the seriousness of the breach of the right to protection of personal data manifests itself in different ways for, on the one hand, legal persons and, on the other, natural persons" the former being "already subject to a more onerous obligation in respect of the publication of data relating to them."[1172]

[1167] For instance, "identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller" (recital 57 of the General Data Protection Regulation (2016/679/EU)).

[1168] Online identifiers include internet protocol addresses, cookie identifiers and radio frequency identification tags, which are provided by the "devices, applications, tools and protocols" of natural persons, and leave traces which are capable of identifying an individual, particularly when "combined with unique identifiers and other information received by the servers" that allow building profiles of such an individual (recital 30, ibid).

[1169] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)* ((Communication) COM (2012) 11 final, 2012).

[1170] *C-92/09 and C-93/09 - Schecke and Eifert*, para 53. That was the case of Schecke and Eifert, where the official title of the partnership identified the natural persons who are its partners.

[1171] Article 29 Data Protection Working Party (2007), *Opinion 4/2007, WP 136*; Mario Viola de Azevedo Cunha, 'The Concept of Personal Data in the Post Lisbon Era: is there Need (and room) for Change?' in Serge Gutwirth et al. (ed), *Data Protection in Good Health?* (Springer 2012).

[1172] *C-92/09 and C-93/09 - Schecke and Eifert*, para 87.

The GDPR lists new categories of personal data meriting reinforced[1173] protection: genetic data,[1174] biometric data[1175] and data concerning health[1176] (articles 4(13), 4(14) and 4(15) of the GDPR). Such data belong in the group of personal data that are, in the words of recital 51 of the GDPR, "by their nature, particularly sensitive in relation to fundamental rights and freedoms". The special category of personal data, often referred to as 'sensitive data', includes "data revealing racial or ethnic origin,[1177] political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (article 9(1) of the GDPR). Article 6 of Convention 108 contains a similarly updated list of sensitive data. Recital 51 of the GDPR clarifies that these "merit specific protection as the context of their processing could create *significant risks* to the *fundamental rights and freedoms*", which leads to the subject of the next sub-section.

2.1.2 THE NOTION OF PROTECTION

Reference to "protection" recalls a duty, vertical and horizontal, to refrain from interfering with the right and ensuring it. In this respect, the second paragraph of article 16 TFEU clearly calls for positive obligations of the EU institutions to adopt legislation to the

[1173] Though intention is not always followed by practice. Spiros Simitis, *Revisiting sensitive data* (Council of Europe, 1999).

[1174] Defined in article 4.13 of the GDPR as data "relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question", namely "chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained" (recital 34).

[1175] Meaning "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".

[1176] Defined as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status". According to recital 35 of the GDPR such data include information "relating to the past, current or future physical or mental health status of the data subject", also those collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU". It includes a "number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test."

[1177] Recital 51 of the GDPR clarifies that "the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races".

effect of concretizing the protection of the right, and it might be seen as producing an obligation to fulfil.

As discussed *supra* (section 1.2.2), as soon as data leave the person to whom they belong, they must be protected. To understand the meaning of protection, it may be useful to refer to (the now suppressed) recital 25 of the Data Protection Directive, to which the Court gave relevance in *Google Spain and Google*. There, the notion of 'protection' is substantiated, among other things, "in the obligations imposed on persons responsible for processing (…)"[1178] (for the notion of processing, see *infra* section 2.2). Although the article is silent about 'duties', protection of personal data is entrusted to the so-called controller and processor (articles 4(7) and 4(8), further specified in Chapter IV of the GDPR). Controller and processor are often the main beneficiaries of the processing of personal data and face corresponding duties, summarized in the principle of 'accountability' introduced by article 5(1) of the GDPR, whereby "the controller shall be responsible for and be able to demonstrate compliance with" the data protection principles".

The general framework for such obligation of protection is contained in article 25 of the GDPR, "data protection by design and by default",[1179] which builds on and elaborates on recital 46 of the Data Protection Directive. One of the messages contained therein is that the data controller must adopt technical and organisational measures necessary to implement data protection principles (listed in article 5, see *infra*) appropriate to the risks[1180] "of varying likelihood and severity for rights and freedoms of natural persons posed by the processing". According to recital 75 of the GDPR, risks

> *"may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their*

[1178] Reporting in full recital 25 in the preamble to the Data Protection Directive. *C-131/12 - Google Spain and Google*, para 67.

[1179] Which reads "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

[1180] Such a risk-based approach derives from article 17 and 20 of the Directive, as well as the approach to sensitive data. Article 29 Data Protection Working Party (2014), *WP29, Statement on the role of a risk-based approach, WP 218*.

rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects."

The Regulation abounds with references to risks,[1181] which can be low, significant or high, and pertain to the rights and freedoms of the data subject or data security. Protection means *securing* any personal data, in the guise of adopting technical and organizational measures commensurate with the risks entailed by the processing. In sum, the idea is that any personal data deserves protection; low risk data will entail easier compliance for the controller, whereas risky processing operations will require the adoption of sophisticated technical and organizational measures.[1182]

2.2 PARAGRAPH TWO: THE *LEX SPECIALIS*, AND SCOPE

Article 8(2) begins with the expression "Such data must be processed…"; it specifies the conditions under which the personal data of individuals can be used[1183] (processed), thus functioning as the *lex specialis* determining the conditions for the enjoyment of such a right. Processing is a term that is understood to encompass 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or

[1181] References to 'risk' are found in recitals 15 (risk of circumvention), recital 24, recitals 28, 38, 65, 71, 74-77, 80, 81, 83, 85, 96, 98, as well as articles 24(1), 25.1, 27(2)(a), 30(5), 32, 33, 35(7)(c)(d) and 35(11), 36, and 39(2). Significant risks are those concerning sensitive data, in recital 51; the regulation refers to high risk in recitals 76, 77, 84, 86, 90, 91 and articles 34 and 35. Finally, data security risks are described in recital 83 of the General Data Protection Regulation (2016/679/EU).

[1182] In this respect, see Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, WP 218, 30 May 2014. For a discussion on risks and the precautionary principle, see Lynskey, chapter 3, and the literature cited therein. Lynskey (2015).

[1183] "Article 8(2) of the Charter thus authorises the processing of personal data if certain conditions are satisfied." *C-543/09 - Deutsche Telekom*, para 52.

combination, blocking, erasure or destruction' (article 2(b) of the Data Protection Directive). The definition of processing, unchanged in the GDPR (apart from 'blocking' which is substituted by 'restriction'), is supplemented by the notions of 'profiling',[1184] and pseudonymisation[1185] (articles 4(4) and 4(5)).

The CJEU clarified that processing includes loading personal data on an internet page (by an individual),[1186] as well as a search engine's finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference,[1187] or making data available in association with names,[1188] even if already published,[1189] and also the record of one's daily work and rest periods.[1190]

The scope of processing is defined, partly *a contrario*, by articles 3 and 4 of the Data Protection Directive, and articles 2 and 3 of the GDPR, with some differences. Here I refer to the GDPR. The protection of article 8 of the Charter does not apply to, *inter alia*: data rendered permanently anonymous;[1191] manual *and* unstructured data files;[1192] data processed in the course of "household activities",[1193] provided that there be no connection with commercial or professional activities (recital 18); data processed outside of the context of the

[1184] "Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

[1185] "Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

[1186] *C-101/01 - Bodil Lindqvist*, para 25; Judgment of 1 October 2015 in Weltimmo, C-230/14, EU:C:2015:639, para 37.

[1187] *C-131/12 - Google Spain and Google*, para 41.

[1188] *C-92/09 and C-93/09 - Schecke and Eifert*, para 58.

[1189] *C-73/07 Satakunnan Markkinapörssi and Satamedia*, paras 48-49.

[1190] Judgment of 30 May 2013 in Worten, C-342/12, EU:C:2013:355, para 19.

[1191] Recital 26 of the Data Protection Directive (95/46/EC). Recital 26 of the GDPR describes anonymous data as "information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. …including for statistical or research purposes." Hence, whoever processes these type of data is lifted from the obligations set out in secondary law (article 11 of the GDPR). On considerations on anonymization, see the Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques* (0829/14/EN WP216, 2014).

[1192] According to recital 15 of the GDPR, "in order to prevent creating a serious risk of circumvention, the … protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

[1193] The latter is controversial, and particularly relevant in the case of Information Society Services (ISSs), as many popular Internet services, such as social networks and web-based emails, currently fall under the household exception's umbrella (but the Lindqvist case and the WP29 interpretation made clear that the Directive would apply when data are made available to a large public). Ronald Leenes, 'Who Controls the Cloud?' (2010) 11 Revista de Internet, Derecho y Politica.

activities of the establishment.[1194] If an establishment is located outside the Union, Union law applies where Member State law applies by virtues of international law (e.g. diplomatic missions and consular posts, recital 25). It also applies when processing relates to 'the offering of goods and services to data subjects in the Union', even if for free, and 'the monitoring of their behaviour', provided this behaviour takes place in the Union. The latter appears in several provisions of the GDPR; to monitor means to track natural persons on the internet, including the possibility of "profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes" (recital 24). In this respect, the Regulation seems to reinforce the finding in chapter 1: personal data can be an important economic resource, but cannot be used at the expense of the person's control over her identity and portrayal of the self.

In the next two sections I analyse the two limbs of article 8(2) which express tenets derived from the FIPs described *supra* in section 1.3, and where consequently the legacy of Convention 108 (and the OECD Privacy Guidelines) is more visible.[1195]

2.2.1 FIRST LIMB OF PARAGRAPH 2

The first limb of paragraph 2 of article 8 of the Charter reads,

> "[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**."

As noted above, this limb identifies the mandatory ("must") substantive principles for legitimate processing that all data processing operations must comply with:[1196] fairness, purpose limitation and lawfulness. These principles are interdependent and cumulative.

First, the processing must be **fair** in accordance with the requirements of article 6a of the Directive (article 5(1) of the GDPR), article 4(1) (a) of Regulation 45/2001, and article 5(1)(a) of the GDPR). Its position in the article confers a double meaning to fairness, which is reflected in secondary law. On the one hand, its position at the beginning of the sentence refers to a general obligation to operate correctly, respecting the principles of data protection

[1194] *C-131/12 - Google Spain and Google*, para 52. According to recital 22 of the GDPR "... Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."

[1195] It should be noted that not all FIPs are part of the formulation, but do nonetheless define the structure of the right in its statutory form.

[1196] See, to this effect, *C-131/12 - Google Spain and Google*, para 71.

as well as the *ordre public* taken as a whole. It is in this sense that the adjective 'fair' sometimes accompanies 'lawful' (in the Data Protection Directive: article 6(1)(a); in the GDPR: article 5(1)(a), 6(2) and 6(4), recital 39 and 45).[1197] On the other hand, fairness also translates into operational principles; Bygrave,[1198] for instance, submits that fairness implies respecting the legitimate interests of the data subject. Indeed, in secondary law, when it is not coupled with 'lawful', fair comes with 'transparent', which is an unspoken, transversal precondition for the three principles mentioned in the limb under analysis. In the same vein, see article 5 (4) (a) of draft Convention 108.[1199] In order to be fair, the purposes of the processing must be evident, and require that the data subject be adequately informed (recital 38, articles 10 and 11 of the Data Protection Directive; articles 11 and 12 of Regulation 45/2001). Similarly, recital 60 of the GDPR states that fair and transparent processing "require that the data subject be informed of the existence of the processing operation and its purposes" (see also recital 39, 42, and 71 of the GDPR, as well as articles 13(2) and 40(2)(a)).[1200] To this effect, articles 12 to 14 of the GDPR contain a specific requirement for the information to be given before data are processed (the information notice).

Second, each processing must relate to a specified, limited purpose (article 6(1)(b) of the Data Protection Directive and articles 4(1) (b) and 6 of Regulation 45/2001; article 5 (1) and (2) of Draft Convention 108). **Purpose limitation** is one of the classic tenets of data protection and has two components: "the data controller must only collect data for specified, explicit and legitimate purposes, and once data are collected, they must not be further processed in a way incompatible with those purposes."[1201] Purpose limitation requires each additional processing to be compatible with the original processing, which implies that the additional operations must be derivable from the original one.[1202] A new purpose is likely to require a new basis for processing.[1203] This applies also diachronically: **storage** should be commensurate to the purpose so that, when the purpose expires, the data should be deleted or rendered unidentifiable (article 5(1)(e) of the GDPR). It is "a pre-requisite for applying

[1197] On the double sense of lawful, as a principle and an obligation, see Article 29 Data Protection Working Party, *Opinion 03/2013 on Purpose Limitation* (00569/13/EN WP 203, 2013).
[1198] Bygrave (2014).
[1199] According to which " Personal data undergoing processing shall be (a) processed fairly and in a transparent manner".
[1200] Unless the purposes fall in one of the exceptions listed in article 13 of the Data Protection Directive (95/46/EC) and 22 of the General Data Protection Regulation (2016/679/EU). In this respect, see *C-473/12 -IPI.*
[1201] Article 29 Data Protection Working Party (2013), *Opinion 03/2013, WP 203*, p. 4. The opinion refers to the Data Protection Directive, but the provision is unchanged in GDPR so, until a different interpretation emerges, it should be valid. Moreover, article 6(4) of the GDPR incorporates most of the suggested changes contained in the Opinion.
[1202] Bygrave (2014); Article 29 Data Protection Working Party (2013), *Opinion 03/2013, WP 203*.
[1203] On the point of compatibility of purposes, see *C-543/09 - Deutsche Telekom*, paras 62-66.

other"[1204] principles relating to the processing of personal data. In fact, purpose limitation is strictly linked with necessity and proportionality (understood as a general principle of EU law and of administrative law[1205]), which entail a reference to suitability[1206] and **minimisation**: the data collected must be adequate, relevant and not excessive (article 6(1)(c) of the Data Protection Directive and article 4(1)(c) of Regulation 45/2001). Article 5(c) of the GDPR substitutes 'non-excessiveness' with the expression "limited to what is necessary in relation to the purposes for which they are processed". Moreover, processing must be legitimate with reference to other areas of law, hence "beyond a simple cross-reference to one of the legal grounds for the processing…Purpose specification under Article 6 [5 of the GDPR] and the requirement to have a lawful ground for processing under Article 7 [6 of the GDPR] are two separate and cumulative requirements".[1207]

Third, the processing must be carried out lawfully, in accordance with either the consent of the person or the law for legitimate purposes (article 7 and 8 of the Directive 95/46, article 5 of Regulation 45/2001, article 6 of the GDPR; article 5(2) and (3) of draft Convention 108). The fact that 'consent' is specifically indicated as a source of legitimacy of the processing is unsurprising; Koops noted that consent is the backbone of the data protection architecture,[1208] understood in terms of informational self-determination. Consent must be freely given, based on sufficient information received about the processing[1209] and adequate in relation to the public receiving it. Consent is strictly linked with fairness and transparency; recital 42 of the GDPR recalls how the definition of consent must use "clear and plain language and it should not contain unfair terms". The GDPR introduces new requirements on consent (article 7), particularly in the case of children below the age of 13 (article 8), whose consent should be provided by the parents or custodians.

Lawfulness is satisfied provided the law is clear and precise, i.e. leaves no room for ambiguous interpretations, and is foreseeable, i.e. the consequences of each provision must be known *ex ante*, "in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights"[1210] (recital 41).

[1204] Article 29 Data Protection Working Party (2013), *Opinion 03/2013, WP 203*, p. 4.
[1205] Bygrave (2014).
[1206] Ibid.
[1207] Article 29 Data Protection Working Party (2013), *Opinion 03/2013, WP 203*, p. 39.
[1208] Koops is very critical of the fact that the GDPR maintains references to consent in the face of today's technological reality. Koops (2014), 'The Trouble with European data Protection Law'.
[1209] Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent* (01197/11/EN WP 187, 2011).
[1210] Which confirms the role of the Council of Europe as the benchmark in the field of the rule of law, as discussed in chapter 1.

Recital 41 of the GDPR also states that reference to a legal basis or a legislative measure "does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned".

2.2.2 *SECOND LIMB OF PARAGRAPH 2*

The second limb of paragraph 2 of article 8 of the Charter reads

> *"Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."*

This limb summarizes the minimum entitlements of individuals *vis-à-vis* their data. It is substantiated in participation,[1211] which gives flesh to the notion of controlling one's data. Secondary law lists additional entitlements to the ones contained in the provision under analysis, such as objection, erasure, notification to third parties and the prohibition of automated individual decisions (article 12 of Directive 95/46 and articles 13 to 19 of Regulation 45/2001). Such omission does not mean that the missing entitlements are irrelevant. To this effect, article 8 of the draft Convention 108 contains a generous list of rights.

An important implicit objective of rectification is to ensure the **accuracy** of the data, i.e. that it is correct and up-to-date (article 6(1)(d) of the Data Protection Directive, article 4(1)(d) of Regulation 45/2001 and article 5(1)(d) of the GDPR): "every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay". Yet, lack of accuracy is not the only grounds for data subjects to claim their rights. In fact, the CJEU clarified that the reference, contained in article 12 (b) of the Directive on rectification, blocking or erasure, to the criteria of incompleteness and incorrectness of the data is not exhaustive. The rights guaranteed in article 12 (b) are conferred on data subjects whenever the processing is incompatible with the

[1211] According to Bygrave (2014), the principle of participation contains four facets, and this limb contains two of them: being able to access one's data, and objecting to the processing thereof (the other two are: being informed about processing operations in general, and consenting after having been provided with sufficient information, which were discussed in the first limb).

Directive, which occurs also when the data are or become inadequate, irrelevant or excessive in relation to the purposes for which they were collected (article 6 (c) Directive 95/46).[1212]

As a result of the *Google Spain* judgment, article 12 (b) is also understood as granting a limited "right to be forgotten" in relation to the indexing of information containing one's name by a search engine, as long as the general public does not have a preponderant interest in accessing the information in question. This decision was codified in article 17 of the GDPR, which includes the entitlements of Regulation 45/2001 (access, rectification, restriction of processing, objection, and automated decisions, articles 15, 16, 18, 19, 20 and 22 respectively), and adds a new one, data portability (article 21).

2.3 PARAGRAPH 3

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

Article 8(3), which is copied verbatim in article 16(2) TFEU, establishes the regime to ensure the protection of personal data and strike a fair balance with the free movement of personal data.[1213] Article 8(3) represents an acknowledgement of the need to take proactive measures for ensuring the right to data protection, thus carving in stone the need for oversight by an independent authority.[1214] The CJEU has clarified that the "establishment in Member States of independent supervisory authorities"[1215] and the control they exercise "is an essential component of the protection of individuals with regard to the processing of personal data",[1216] in that it derives from EU primary law.[1217]

The paragraph refers to and is specified by articles 28 of Directive 95/46 (and recitals 62 and article 29[1218]), whereby Member States must establish one or more public authorities responsible for monitoring the application of the Directive, and endowed with consultative

[1212] *C-131/12 - Google Spain and Google*, paras 70 and 92.
[1213] Judgment of 8 April 2014 in Commission v. Hungary, C-288/12, EU:C:2014:237, para 51.
[1214] Judgment of 16 October 2012 in Commission v. Austria, C-614/10, EU:C:2012:631.
[1215] Referring also to C-518/07 (§ 23) and C-614/10 (§ 37). *C-288/12 - Commission v. Hungary*, para 48.
[1216] *Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*, para 68.
[1217] *C-288/12 - Commission v. Hungary*, para 47.
[1218] Article 29 of the Directive created the Data Protection Working Party on the protection of individuals with regards to the processing of personal data (hereafter Article 29 Working Party), tasked *inter alia* with the interpretation of the "questions covering the application of the national measures adopted under the Directive" with a view to its homogeneous application. The Article 29 Working Party issues Opinions, which greatly contribute to the understanding of the Directive. It complements the work of national data protection authorities envisaged by article 28 of the Directive.

powers with regards to administrative measures or regulation concerning data protection. The paragraph is further specified by Regulation 45/2001 establishing the European Data Protection Supervisor (EDPS), tasked with 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. The GDPR contains a definition of supervisory authority that reinstates the requirement of independence (article 4(21)), further specified in article 52.

3 THE ATTRIBUTES OF ARTICLE 8 OF THE CHARTER

I first attempted to identify attributes of the right to the protection of personal data as understood in the Union in the context of the SURVEILLE project.[1219] It is apt to recall that attributes are the smallest components of a right; here they will be used to gain in granularity when analysing the impact that technologies used in connection to cybersecurity have on privacy rights. Attributes may have a core or essence, which represents a sub-element of the attribute which, if violated, would necessarily imply the violation of the whole right.

The purpose of this section is to refine my first attempt to identify attributes, similarly to that done for the right to private life, with the caveat that this procedure is more experimental than that followed in chapter 4.[1220] At the same time, this exercise benefits from the well-established discussion of principles of personal data, so that, in essence, this section broadly specifies those principles that are attributes of the right as enshrined in the Charter. Moreover, as discussed in chapter 4, the legal framework of reference being EU law, the attributes are specific to the Union legal framework, and hence I have no pretence as to their universal application.

[1219] Porcedda (2013), *Paper Establishing Classification of Technologies on the Basis of their Intrusiveness into Fundamental Rights* (SURVEILLE Project Deliverable D 2.4).

[1220] A similar exercise was hypothesized by Tzanou (2012) based on the following quote: "Using directive 95/46/EC as a starting point, and bearing in mind the provisions of other international data protection texts, it should be possible to arrive at a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate. Such a minimum list should not be set in stone." Article 29 Data Protection Working Party, *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive (Working Document),* (DG XV D/5025/98 WP 12, 1998). Yet, Tzanou fell short of proposing cores, and only made two examples: strict conditions for processing sensitive data (as the core of sensitive data), and the prohibition of secondary use (as the core of purpose specification).

In order to identify the attributes, which should be as few as possible, mutually exclusive, and capable of capturing the full meaning of the right, I have discerned the applicable legal framework. As anticipated in section 1, the content of the attributes is distilled from the principles mentioned in article 8 of the Charter – derived from Convention 108 and the Data Protection Directive and specified by the GDPR as the latest expression of the fundamental right – as interpreted by the judgments of the CJEU (ECJ and General Court) *after the Charter acquired primacy* with the entry into force of the Lisbon Treaty (hence since December 2009).[1221] As discussed in section 1.5, reliance on secondary law is justified by the fact that it extensively refines the purview of a Treaty-based right. Moreover, I refer to the draft revised Convention 108, under the understanding that, even if the instrument will be relied upon solely to decide the adequacy of the legislation of third countries with a view to allow data transfers, its content provides important insight into what represents a minimum threshold of the right (see *supra*, section 1.3.1). Finally, I occasionally refer to data protection principles contained in recent literature, in particular the latest formulation of the principles proposed by Bygrave.[1222]

The CJEU last reaffirmed in *Schrems* that the control performed by an independent authority is an essential component of the right, because it is listed in the definition of the right.[1223] By analogy, all elements contained in the definition should be considered an essential component of the right. Furthermore, in *Google Spain and Google* the Court declared that the requirements of article 8(2) and 8(3) of the Charter "are implemented *inter alia* by Articles 6, 7, 12, 14 and 28 of Directive 95/46", which specify further principles. Here I refer to the principles formulated in the GDPR, which will be prospectively enforced. Moreover, in *Digital Rights Ireland* the ECJ identified an essential component of the right, which is not part of the definition, but stems from secondary law and the old Convention 108. Hence, it is possible to identify elements of secondary law that, due to their importance, can be seen as attributes of the right. Such a finding is reinforced by their inclusion in the draft Convention 108.

[1221] Such limitation is justified by the fact that, until the Charter acquired primacy, the Court did not analyse cases concerning the protection of personal data under the light of article 8 of the Charter, limiting itself to references in passing.

[1222] He identifies seven tenets: i) fair and lawful processing; ii) proportionality; iii) minimality; iv) purpose limitation; v) data subject influence; vi) data quality; and vii) sensitivity. While his analysis has the advantage of making wide reference to the EU legal framework, his definition cannot be used as a reference because it is construed in such a way as to reflect an international understanding of the concept, rather than as an EU right. Bygrave (2014).

[1223] *C-362/14 - Schrems*, para 41.

Hence, the first step consists in drawing a comparison between the data protection principles identified in section 2 on the formulation of the right, and summarized in the table below. The top row contains the principles, and the expression 'FIP' in brackets indicates that it is a fair information principle (accompanied by the original name when relevant). The left column refers to article 8 and the GDPR. The presence of the principle in the relevant legal instrument is signalled with the dummy variable "X" (no value means absence).

Principles/ Instrument	**Fairness**	**Lawfulness/consent**	**Purpose limitation (FIP)**	**Use limitation (FIP)**	**Collection limitation (FIP)**	**Transparency (FIP openness)**	**Individual rights (FIP participation)**	**Accuracy (FIP data quality)**	**Accountability (FIP)**	**Independent control**	**Integrity and confidentiality (FIP security)**
Article 8 of the Charter	X	X	X			X if with fairness	X				
GDPR	X (art. 5.1(a.)	X (art. 5.1(a.)	X art. 5.1(b) and (e)		X (art. 5.1 (c)	X art. 5.1(a)	X	X Art. 5.1(d)	X art. 5.2	X	X art. 5.1(f)

Table 17 Comparison of data protection principles

Here it is apt to recall that attributes should be as few as possible, mutually exclusive, and capable of capturing the full meaning of the right. As a result, not all existing principles must necessarily be translated into independent attributes. I shall now take a step back to the discussion on PIAs of chapter 5 (section 3.2); that is, an exercise sharing common goals with the search for attributes. Some time ago De Hert[1224] appraised the possibility of building a data protection impact assessment (IA). He concluded that, while the nature of the right to data protection hindered the conclusion of a real IA, it was possible to carry out a compliance check based on the requirements laid down in legislation. He then listed some of the classic principles, or FIPs (with no explicit reference to them), namely: legitimacy, purpose restriction, security and confidentiality, transparency, data subject's participation and accountability.

[1224] De Hert (2012).

While I contest De Hert's conclusion, whereby it is not possible to perform impact assessment for data protection, I recognize the partial relevance of compliance checks. As acknowledged by Bygrave,[1225] one of the sources of data protection is to be found in the rule of law. Such a source is visible in the formulation of FIPs and the ensuing first limb of article 8.2 of the Charter (see *supra*, section 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.*" Hence, those elements that derive from the rule of law, namely fairness, purpose limitation and lawfulness, as well as independent oversight, will have more the character of a compliance check.

I propose the attributes summarized in the table below. I will justify the choice in the sections where I describe the attributes.

Attributes that come from article 8	**Attributes identified by the Court (found in secondary law and Convention 108)**	**Attributes that do not originate from the formulation, but are found in secondary law and Convention 108**
Legitimate processing • Fairness/transparency • Purpose limitation • Lawfulness	Security	Data accuracy and minimization
Oversight (partly rule of law) Independent	← →	Human control (automated decisions)
Data subject's rights: • Access • Rectification • Objection, including profiling • Erasure (right to be forgotten) • Portability • Restriction		

Table 18 Sources of attributes

[1225] Bygrave (2014).

3.1.1 LEGITIMATE PROCESSING (ATTRIBUTE OF THE RULE OF LAW)

This attribute concerns the expectation of the data subject to the overall legitimacy of the data processing, and stems from the first limb of article 8(2) of the Charter: "Such data must be processed fairly for specified purposes on the basis of the *consent* of the person concerned or some other legitimate *basis* laid down by law". It encompasses the three principles expressed therein: fairness, purpose specification and lawful processing. I treat storage specification as a component of purpose specification: since storage is a distinct processing operation, it must respect the objective of purpose specification and limitation. The three principles pave the way to a single attribute because they are not mutually exclusive, but rather cumulative. This is due to their common roots in the rule of law, which effects functional interconnections. In detail, fairness stems from legal certainty (and lawfulness), purpose specification from proportionality and non-arbitrariness, and lawful processing from legality.

Secondary law and interpretations thereof highlight such interconnections. First, article 5(1) (a) of the GDPR states that personal data must be "processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)". Article 6 of the GDPR on conditions of lawfulness[1226] clearly refers to purpose specification and fairness. Paragraph 3 clarifies that

> *"…The purpose of the processing shall be determined in [the] legal basis or… shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member*

[1226] In connection to the legitimate aim of the controller, the ECJ ruled that "The processing by a search engine can be considered legitimate under [the ground regulation] the legitimate interests of the controller, but that ground … necessitates a balancing of the opposing rights and interests concerned, in the context of which account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter." *C-131/12 - Google Spain and Google*, para 74.

State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued."[1227]

Likewise, the conditions whereby processing operations other than those for which the personal data have been collected are compatible with the original purpose[1228] (specified in article 6(4) of the GDPR which follows the recommendations issued by the Article 29 Data Protection Working Party[1229]), clearly connect with specification, fairness and consent. Recital 50 of the GDPR clarifies that further processing operations "should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected."[1230] Moreover, in order to ascertain the compatibility of a further processing with the original purpose, the controller must first meet "all the requirements for the *lawfulness* of the original processing" and should take into account "any link between those purposes and the purposes of the intended further processing" and "the context in which the personal data have been collected, in particular the *reasonable expectations* of data subjects based on their relationship with the controller as to their further use". With regards to purpose limitation, the Article 29 Data Protection Working Party noted that it is "preliminary to several other data protection tenets and contributes to "transparency, legal certainty and predictability", which in turn enable control by the data subject".[1231] Furthermore, the Working Party submits that the purpose must be legitimate (as discussed *supra*, section 2.2.1), specific and explicit to both controller and data subjects, thus encapsulating fairness. Hence, a purpose that is vague or general, such as 'improving users' experience', or 'marketing purposes' will not fulfil the requirement of specificity. As the Court declared in *Digital Rights Ireland*, using data for several purposes without the data subject "being informed is likely to

[1227] See, in this respect Worten, where the Court ruled that "national legislation…which requires an employer to make the record of working time available to the national authority responsible for monitoring working conditions" is not precluded. *C-342/12 - Worten*.

[1228] See also *ASNEF* and *FECEDM*, where the Court ruled that further processing of personal data in the absence of consent cannot be limited to data that are already available in the public domain. *Joined cases C-468/10 and C-469/10 - ASNEF and FECEDM*.

[1229] Article 29 Data Protection Working Party (2013), *Opinion 03/2013, WP 203*. According to WP29, the legislator prohibits incompatibility; hence, it is incompatibility which is the focus of attention. All other processing operations are permissible so long as they are compatible, globally legitimate/fair and lawful. A different purpose may not necessarily be incompatible, and the assessment must be substantive and on a case-by case basis.

[1230] Hence "the passing of the same data to another undertaking intending to publish a public directory without renewed consent having been obtained from that subscriber is not capable of substantively impairing the right to protection of personal data, as recognised in Article 8 of the Charter". Judgment in *C-543/09 - Deutsche Telekom*, para 66.

[1231] Article 29 Data Protection Working Party (2013), *Opinion 03/2013, WP 203*, p. 11.

generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[1232]

The provisions on consent also link to fairness and purpose limitation. Pursuant to article 4(11) of the GDPR, consent[1233] is defined as "any freely given, *specific*, *informed* and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." Recital 32 of the GDPR further specifies that "…Consent should cover all processing activities carried out for the *same purpose* or purposes. When the processing has *multiple purposes*, consent should be given for all of them." Consent has to be assessed in the light of the whole Regulation, in that, pursuant to article 7(2) of the GDPR, "consent given in the context of a written declaration…which constitutes an infringement of this Regulation shall not be binding". Moreover, "where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data" (article 7(1) of the GDPR).

On the basis of the applicable law just expounded, the functional interconnection of the three principles can be easily explained. If a processing is not fair, then there is no guarantee of purpose limitation, which would void consent or challenge lawfulness. If the purposes of the processing are indeterminate, then the processing cannot be fair, paving the way to uninformed consent and a general disrespect of lawfulness. If the processing is carried out without consent or pursuant to the wrong legal basis, then it is unfair, and there is no guarantee that the purpose is specified and limited as expected.

Perhaps the case lending the strongest support to this attribute is *Digital Rights Ireland*,[1234] where the court said, in relation to the Data Retention Directive[1235] (focussing on storage limitation) that "the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data". In other cases the CJEU focussed more on the links between lawfulness and other principles concerning the protection of personal data. In relation to this

[1232] *Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*, para 37.
[1233] The court ruled that denial of consent to transfer (process) one's data can only be overruled if the potential controller establishes the necessity of such processing (in relation to one of the grounds for lawful processing). *C-28/08 P - Bavarian Lager Ltd.*, para 77.
[1234] *Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*, para 54.
[1235] Data Retention Directive (2006/24/EC).

attribute, I should recall the findings in *Google Spain and Google*,[1236] whereby, under certain conditions, "even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed."

***

In sum, this attribute refers to the expectation of the data subject that the processing must be legitimate, in all senses of the concept of legitimacy: in relation to data protection law as a whole (fairness), the interests of the controller in pursuing the processing (purpose limitation), and the legal system/*ordre public* as a whole (lawfulness). Hence the attribute is called 'legitimate processing'.

3.1.2 OVERSIGHT

This attribute refers to the availability of oversight to ensure the respect of the principles relating to the processing of personal data. It is composed of two elements. The first, distilled from article 8(3), refers to the availability of an independent public authority monitoring compliance with data protection laws. Similarly to the previous attribute, it has a strong basis in the rule of law, particularly in the availability of independent courts and effective remedy, and as such it is likely to remain unaffected by the conditions attached to technology; rather, it will be influenced by the legal terms and conditions attached to a specific technology.

The second is derived from secondary law and does not correspond to any existing principles of personal data protection, but, as I explain below, refers to the heart of the value of personal data expounded in chapter 2 (section 3.3.2). Moreover, it finds strong support in the draft revised Convention 108.

[1236] *C-131/12 - Google Spain and Google*, para 93.

3.1.2.1 Independent supervisory authority

Supervisory authorities are conceived as the guardians of "the right to privacy";[1237] this is "an essential component of the protection of individuals with regard to the processing of personal data"[1238] because it is enshrined in "primary law of the European Union, in particular Article 8(3) of the Charter and Article 16(2) TFEU".[1239]

According to article 4(21) of the GDPR, a supervisory authority is an independent public authority that is established by a Member State. Whereas Member States are free to choose the most appropriate institutional model for the authority,[1240] "independence" is a fundamental attribute of a supervisory authority.[1241] The ECJ specified essential criteria in three cases where the Commission sued Germany, Austria and Hungary for failure to fulfil obligations. Essential criteria for independence are the absence of directions and instructions, but also of political influence (including the threat of early termination), which could lead to "prior compliance" or partiality.[1242] Such criteria have been embedded in articles 51 and 52 of the GDPR. Moreover, in *Schrems* the Court clarified that independence, which is intended to ensure the "effectiveness and reliability of …the protection of individuals" (§ 41) extends in relation to the Commission, in that a DPA "must be able to examine" the adequacy of a transfer of data (in the context of hearing a claim lodged by a person with reference to such transfer) even if the Commission has already issued a decision pursuant to article 25(6) of the Data Protection Directive (§ 53). To impede the assessment of adequacy in this way would mean depriving individuals of their right to a claim.

The provisions on independence serve the ultimate task of supervisory authorities, namely to ensure the appropriate application of data protection rules in order to safeguard data subjects' rights and enable the free flow of personal data. Case law suggests that for monitoring to be ensured, the data should be stored in the European Union.[1243] In order to carry out their tasks, authorities are endowed with powers; those endowed by Directive 95/46 are non-exhaustive. According to the Court, besides "investigative powers, such as powers to collect all the information necessary for the performance of their supervisory duties, and

[1237] *Case C-614/10 - Commission v. Austria*, para 52.
[1238] *C-362/14 - Schrems*, para 41.
[1239] Ibid, para 40.
[1240] *C-288/12 - Commission v. Hungary*, para 68.
[1241] The ECJ specified that "the words 'with complete independence' in the second subparagraph of Article 28(1) of Directive 95/46 must be given an autonomous interpretation, independent of Article 267 TFEU, based on the actual wording of that provision and on the aims and scheme of Directive 95/46 (see Commission v. Germany, paras 17 and 29)." *Case C-614/10 - Commission v. Austria*, para 40.
[1242] *C-288/12 - Commission v. Hungary*, paras 51-54.
[1243] *Joined cases C-293/12 and C-594/12 - Digital Rights Ireland*, para 68.

effective powers of intervention, such as powers of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, or of warning or admonishing the data controller", authorities should also have "the power to penalise the data controller by imposing on him, where appropriate, a fine".[1244] The GDPR codified such findings in article 58, which harmonizes the powers of supervisory authorities across the Union.

***

In sum, this attribute concerns the potential and actual possibility, for the data subject, to refer to a public and independent supervisory authority in order to have his or her rights protected.

3.1.2.2 Human intervention

This attribute concerns the right of a natural person to have another natural person, rather than a machine, take decisions based on the processing of personal data affecting a data subject. Such an individual could be the Data protection officer (article 37 of the GDPR) or any data controller. While this attribute is rooted in secondary law, particularly in article 15 of Directive 95/46, it nonetheless expresses one of the key values of personal data protection discussed in chapter one. Article 15 of the Directive 95/46, read in the light of recital 41, mandates that automated processing of data intended to evaluate certain personal aspects relating to the data subject, such as one's performance at work, creditworthiness, reliability, conduct, etc. cannot be the sole basis for taking decisions that produce legal effects concerning the data subjects, or which otherwise significantly affect them. When such decisions are taken pursuant to the exception of this norm, the data subject is entitled to know the logic involved in such automatic processing of data in order to put forward his or her point of view, and appropriate safeguards must be put in place. In *Schrems* the ECJ followed the reasoning of *Digital Rights Ireland* when it declared that the need to "lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards…. is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data".[1245]

[1244] *C-230/14 -Weltimmo*, paras 48-49.
[1245] *C-362/14 - Schrems*, para 91.

This attribute and its rationale is intimately linked with the attribute 'data subjects' rights', particularly the right to object. The rationale for subjecting automated decisions to heightened controls is that decisions based on automated processing stem from a partial depiction of the individual, which is based on the expropriation of control over identity and (digital) personality. Indeed, the draft Article 8 (a) of the revised Convention 108 recognizes this entitlement. The GDPR devotes a number of articles and recitals to the subject matter. Article 22 of the GDPR, which is based on article 15 of Directive 95/46, reiterates the generic prohibition on taking decisions which produce legal effects or significantly affect a data subject when based solely on automated processing, and a reinforced prohibition on taking such decisions when based on the automated processing of special categories of personal data. Recital 71 of the GDPR recommends such decisions not to concern a child (in the GDPR, a child aged 13 or under), and offers examples of the negative effects of such decisions on the data subject, e.g. "automatic refusal of an online credit application or e-recruiting practices without any human intervention".

Article 22.2 provides for exceptions to the general prohibition, e.g. "for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent" (recital 71). In this case, pursuant to article 22(3) of the GDPR, the controller must provide safeguards consisting *at least* in ensuring "the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision". This requirement has the potential of expressing the **core**, or essence, of this attribute, the infringement of which constitutes a violation of the right. The provision of information on such automated processing, which is formulated in the guise of a recommendation in recital 71,[1246] is actually mandatory pursuant to articles 13(2)(f), 14(2)(g) and 15(1)(h), which is consistent with the general obligation of fairness and transparency. The controller must inform of "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about

[1246] Recital 71 reads "… In any case, such processing *should* be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention (…). (…) In order to ensure fair and transparent processing in respect of the data subject…the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised…and that prevents, inter alia, discriminatory effects on natural …or that result in measures having such an effect." (emphasis mine).

the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" (see also recital 63 of the GDPR).

An important innovation of article 22 of the GDPR, compared with article 15 of Directive 95/46, is the explicit reference to profiling, which is defined in article 4(4) of the GDPR (and recital 71) as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements" (see also article 3(4) of the AFSJ Directive). Recital 72 clarifies that profiling "is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles" and that the future European Data Protection Board should issue suitable guidance.

Profiling, in turn, presupposes monitoring the behaviour of data subjects, which, according to recital 24 of the GDPR, consists in tracking data subjects[1247] (on the internet), irrespective of the objective of such tracking.

The negative change, compared with Directive 95/46, is that article 22 of the GDPR is subject to the restrictions set by article 23, as opposed to article 15 of Directive 95/46, which was not subject to such restrictions. However, Directive 95/46 had limited reach. The new Directive on data processing in the AFSJ reiterates the prohibition of decisions based solely on automated processing, and the right to obtain human intervention, in article 11 and the corresponding recital 38. In general, the GDPR contains several references to monitoring, profiling and automated processing.[1248]

Automated decisions based on profiling, moreover, trigger the obligation to conduct an impact assessment (article 35(3)(a)), as does "monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects

[1247] The recital refers to the Internet in that it concerns data controllers that are not established in the European Union.

[1248] Profiling is mentioned in recitals 24, 27, 38, 63, 70, 71, 72, 73, 75 and 91, and articles 13(2) (f), 14(2)(g), 15(1)(h), 21(1-2), 22(1) and (3), 35(3)(a). Automated (or automatic) decisions can be found in recitals 24, 63, 71, 75, and articles 13(2) (f), 14(2)(g), 15(1)(h), 22(1) and (3), 35.(3)(a). References to monitoring behaviour are contained in articles 3(2)(b), 27(3), 35(3)(c), 35(6), and recitals 24, 71, 80, 91, 97 (monitoring epidemics are in recitals 46, 52 and 53).

from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale" (recital 91).

***

In sum, this attribute concerns the right of an individual to have another natural person, rather than a machine, taking decisions affecting a data subject based on the processing of personal data. Its core could be identified in the provision whereby the data subject must be able to request human intervention on the part of the controller, to express his or her point of view and to contest the decision. This attribute is closely linked to the right not to be characterized solely by a machine (see *infra*, section 3.1.3). Its relevance is connected to the importance of retaining control over the portrayal of one's identity to society, and the consequences that can ensue.

3.1.3 DATA SUBJECT'S RIGHTS

Data subject's rights are the last attribute stemming directly from the definition of the right in the Charter. The attribute gives substance to the notion of control over one's personal data. Article 8(2) of the Charter mentions the rights of access and rectification. In line with the interpretation given by the Court in *Google Spain,* that the requirements of article 8(2) of the Charter "are implemented *inter alia* by Articles 6, 7, 12, 14 and 28 of Directive 95/46", the corresponding articles of the GDPR implement and further specify the content of this attribute. Hence, this attribute means that the individual has, as a general rule, at least six entitlements, subject to the restrictions embodied in article 23 of the GDPR. The draft revised Convention 108 recognizes most of them, with the exception of the right to portability and rectification. Such entitlements vary in the degree of intensity, and relate to each other as preliminary and subsequent steps, or alternative steps, of a strategy geared at controlling one's data.

First, data subjects enjoy the right of access, i.e. to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, to obtain a free copy[1249] of personal data being processed (art. 1

[1249] Hence the interpretation given by the Court in X may be tenable only in part: "In view of the considerations made above in the analysis of Question 2, Article 12(a) of Directive 95/46 must be interpreted as requiring

GDPR), if possible via electronic means (see also draft article 8(1) (b) of revised Convention 108). This is particularly the case with health data (recital 63). Such a right to information includes notification of the appropriate safeguards that attach to data transferred outside of the Union. Such a right finds its limits in the potential negative effects on the rights or freedoms of others, including trade secrets or intellectual property, and in particular copyright protecting software (recital 63). This includes, for an applicant for a residence permit, access to all data processed by the national administrative authorities in the guise of a full summary of those data in an intelligible form (allowing that applicant to understand those data and check their accuracy and processing in compliance with that directive), so that the applicant can potentially exercise the other rights conferred by secondary law.[1250]

Second, the data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her (article 16 of the GDPR; draft article 8 (1) (e) of revised Convention 108). Differently from the Directive, the interpretation given by the Court in *Google Spain*, and the draft Convention 108, such a right seems now to limit rectification to the incorrectness of the data, whereas the rectification becomes optative if the stored data "infringes the Regulation or Union or Member State law to which the controller is subject" (recital 65). However, in cases in which the processing is unlawful, then the data subject can claim a stronger entitlement, that of erasure.

This third entitlement of the data subject (the so-called "right to be forgotten" of jurisprudential origins), means that the data subject has a right, under specific conditions, to request and obtain the erasure of personal data concerning him or her without undue delay, particularly when the data subject withdraws consent, the data are no longer necessary, or the processing is or becomes otherwise unlawful (as in *Google Spain and Google*, discussed *supra,* section 2.2.2). Recital 65 clarifies that such a prerogative is particularly important in the case of data subjects who are, or were, children, at the time of the processing of their personal data. If the controller has publicly disclosed such data (or to specific recipients, article 19 of the GDPR), it has an obligation to take reasonable steps to inform any controllers of such data of the data subject's request to erase such data and any copy thereof. This obligation, however, has to be commensurate with the costs of implementation and available technology, and must be reconciled with the right of freedom of expression and information, reasons of public interest in the field of public health, archiving purposes in the public

Member States to ensure that the exercise of that right of access takes place without constraint, without excessive delay, and without excessive expense". *C-486/12 - X*, para 25.

[1250] *Joined cases C-141/12 and C-372/12 - YS and others*.

interest, scientific or historical research purposes or statistical purposes, and to fulfil a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The draft Convention 108 recognizes a generic right of erasure when data are processed contrary to the provisions of the Convention (draft article 8 (e)).

The fourth entitlement consists in requesting the restriction of processing (what was 'blocking' in Directive 95/46). Restriction means "the marking of stored personal data with the aim of limiting their processing in the future" (article 4(3) of the GDPR), for instance by "temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website" (recital 67). Such a restriction can be demanded, pursuant to article 18 of the GDPR, in cases where the data subject has requested the rectification of their personal data, during the time necessary to verify their accuracy, or similarly when the data subject has objected to processing (see *infra*), during the time necessary to ascertain whether the legitimate interests of the controller can override the rights of the data subject; as an alternative to the erasure of unlawfully processed data, for instance because the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims. In this case, the only processing allowed is storage, unless the data subject requests to lift such restriction, or some restrictive conditions apply (article 18(3)).

The fifth entitlement is new, and consists of "receiving the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided", where the processing is performed on grounds of consent and also by automated means (article 20 of the GDPR). Although the so-called right to portability does not lay down an obligation to develop interoperable processing systems, recital 68 encourages data controllers to use compatible formats for data transfers, particularly to enable the direct transfer from one controller to the other (article 20(2)). Article 20 provides for the independence of the right to portability and the right to erasure, which should not be mutually prejudicial.

The final entitlement, already contained in the Directive 95/46 and interpreted by the Court in *Google Spain and Google*[1251] and *Bavarian Lager Ltd.*, enables the data subject to object to processing on grounds relating to the particular situation of the data subject, when automated processing relates to the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or to the legitimate interests pursued by the controller[1252] or by a third party (articles 6(1)(e) and (f), and 21 of the GDPR). Pursuant to article 21 of the GDPR, read in the light of recitals 69 and 70, data subjects are endowed with the prerogative of objecting to the automated processing of personal data consisting in profiling, including for marketing purposes[1253] (with limits consisting, for instance, in ensuring public health[1254]). The innovation, compared to the corresponding article 14 of Directive 95/46, is that the former referred to direct marketing, whereas the GDPR refers widely to profiling (based on article 6(1)(e) and (f)), a point that was anticipated in the discussion on human intervention (*supra*, section 3.1.2.2). In this particular connotation, objecting to the processing means allowing an individual not to be characterized solely by a machine. The draft article 8 (d) of the revised Convention 108 incorporates these innovations.

In addition to that discussed *supra*, section 3.1.2.2, the explanation to this attribute is contained in two recitals of the GDPR. According to recital 75 (quoted also in section 2.1.2) "… where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles", there is a "risk to the rights and freedoms of natural persons" which could lead to "physical, material or non-material damage". It is in this light that profiling of children is inadvisable, as they "may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data" (recital 38 of the GDPR).

***

[1251] "As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question." *C-131/12 - Google Spain and Google*.

[1252] As for the legitimate interests of the data subject prevailing over those of the data controller, in the context of access to freedom of information, see *C-28/08 P - Bavarian Lager Ltd.*, para 77.

[1253] Pursuant to article 6.1(f) and recital 47, marketing is considered a legitimate interest of the data controller, which can nonetheless be overridden as described in the main text.

[1254] Recitals 46, 52, 53 of the General Data Protection Regulation (2016/679/EU).

Hence, this attribute is substantiated in the control exercised by natural persons on their own personal data, which can be exercised through six different avenues. Such entitlements vary in the degree of intensity, and relate to each other as preliminary and subsequent steps, or alternative steps, of a strategy geared toward controlling one's data. Hence, following access, an individual could (resort to restriction with a view to) either demand rectification or to object to the processing; or could request the portability of his or her personal data and, as a more drastic measure, their erasure.

No case law has, thus far, given indication of a potential core. Here I propose two candidates: the first is access, without which no further action can be taken; the second is objecting to profiling, understood as the retention of the individual over his or her identity and personality, the importance of which was discussed in chapter 2.

3.1.4 MINIMIZATION AND ACCURACY

This attribute does not derive directly from the definition of the right, but descends logically from the previous attribute, and has strong links with the attributes 'legitimate processing' seen above (*supra*, section 3.1.1) and security (*infra*, section 3.1.5). It encompasses two principles of personal data protection, which it is appropriate to examine together, as one is a consequence of the other. It expresses the need to collect the minimum amount of personal data possible and, within this category, maintain the data accurate and up-to-date. Such principles are now codified in the draft revised Convention 108.

The first principle is minimization, whereby the data processed must be those that are "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Article 5(c) of the GDPR; draft article 5(4)(c) of revised Convention 108). Data minimization concretizes the undergirding idea of data protection, whereby data should not be processed, unless this is unavoidable, and hence is one additional way to provide control for the individual. Data minimization is intimately connected to security (see *infra*, section 3.1.5), in that security increases when fewer data are processed, for the simple reason that fewer data are exposed to risks. It also links to legitimacy and purpose limitation, in that a suitably carved identification of purposes leads to a more targeted collection of personal data.

Moreover, in a passage of *Google Spain and Google* that I have already referred to, the Court declared that initially lawful processing of accurate data "may, in the course of time,

become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed."[1255]

This passage allows for linking data minimization with the principle of accuracy, whereby data must be indeed accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay" (article 5(d) of the GDPR; draft article 5(4)(d) of the revised Convention 108). The link with the attribute of data subjects' rights should be immediate, in that one of the objectives of participation is to either verify accuracy or redress obsolete data. Furthermore, reference to purposes links to the idea of purpose specification. In *Digital Rights Ireland*, the Court considered "the obligation to erase or make those data anonymous where they are no longer needed for the purpose of the transmission of a communication" to be an important element of the "the system of protection of the right to privacy established by" secondary law "with regard to the processing of personal data in the electronic communications sector" (ground 32). The importance of accuracy can be once more best understood in relation to the 'personal' criterion of data protection, which links it with a persona and her identity. To maintain accuracy means to respect and reflect the individual's uniqueness, giving relevance to the individual behind the piece of information. The importance of accurate data transcends the field of personal data protection. In the case of *U* (which concerns private life), the ECJ noted that for the information in a "machine readable personal data page of a passport" to be "effectively verifiable by the authorities of those States, the form in which the various components of the name of the holder appear must be free of any ambiguity and, therefore, of any risk of confusion" and therefore "those requirements are not satisfied where, in a passport, the birth name of the holder entered there is indicated by means of an abbreviation which is, moreover, not translated into one of the languages required." (§ 44 and 47).

Data must be, first, as few as possible and then, within such pool of data, they must be maintained accurate. Data which are inaccurate become inadequate and hence, in the language of recital 39, "every reasonable step should be taken to ensure" that they are rectified, as seen above, whereas data which are outdated become irrelevant, and hence must be erased.

[1255] *C-131/12 - Google Spain and Google*, para 93.

Thus far, the Court has not pronounced itself yet on the possibility of a core in relation to this component of the right to personal data protection.

***

This attribute, which is strongly related to purpose specification, data subjects' rights and security, embodies an additional element of control of personal data, whereby individuals should have requested of them the minimum amount of personal data possible for a given purpose and that, within this category, the link between the information and the uniqueness of the individual should be maintained, in the guise of accurate and up-to-date data.

3.1.5 SECURITY: ATTRIBUTE AND CORE

As described in section 2.1.2, the notion of protection means securing data against risks stemming from their processing. If references to security can only be indirectly obtained from the definition of personal data, then it was the Court that gave it the status of a principal component of the right. In ground 40 of *Digital Rights Ireland* the Court identified, *a contrario*, the adherence to data security with a core of personal data

> *"Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter, because Article 7 of Directive 2006/24 provides, in relation to data protection and data security, that ... Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data."*

Hence there is an overlap between security as an attribute and as a core of personal data protection.[1256] The GDPR acknowledges this status by including security among the data protection principles ('integrity and confidentiality'). This is substantiated in the expectation (and parallel obligation) that the controller implements appropriate measures against the risks of varying likelihood and severity for the rights and freedoms of natural persons (articles 5(f) and 32 of the GDPR; see also draft articles 7 and 8 *bis* of the revised Convention 108).

[1256] It must be noted that the Court applied its reasoning in an unsteady manner, in that it first argued that the Data Retention Directive did not impinge on the essence of the right and then, in ground 66, held that the Directive "does not provide for sufficient safeguards…in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality", and in ground 67 said that it "does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply".

Indeed, as mentioned *supra* (section 2.1.2), security measures are geared at protecting against a host of risks. Some risks, listed in the aforementioned recital 75, are inherently tied to the nature of the processing, such as where the processing may: give rise to discrimination, damage to the reputation, or loss of rights and freedoms; concern sensitive information or children; effect profiling; or involve a large amount of personal data and affect a large number of data subjects. Other risks are tied to the security of the data. Article 5(f) contains an indicative and non-exhaustive list of the risks, i.e. unauthorised or unlawful processing and against accidental loss, destruction or damage, which is complemented by recitals 75 and 83: for instance, identity theft or fraud, financial loss, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, accidental or unlawful alteration of data, which "may in particular lead to physical, material or non-material damage".

The attribute is substantiated in particular in the expectation that appropriate technical and organizational measures are taken, as anticipated in chapter 2 (section 3.3.2), 3 (section 1.2.2) and 4 (section 1). Examples of such measures are provided in article 32, and include pseudonymising and encrypting personal data, ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services; in case of an accident, swiftly restoring the availability and access to personal data, and regularly testing, assessing and evaluating the effectiveness of technical and organisational measures implemented.

In sum, this attribute means that the individual can trust that personal information is protected against risks of varying nature and likelihood which could lead to physical, material or non-material damage of the data themselves and their rights and freedoms. This attribute has been clearly identified as an essential component of the right, and must therefore be seen as a core.

3.1.6 Considerations on sensitive data

Bygrave looks at the protection of sensitive data as an essential component ('core principles') of the right to the protection of personal data.[1257] Thus far, the Court has not

[1257] Bygrave (2014), chapter 5, pp. 145-167.

directly addressed the matter of sensitive data in the field of personal data protection. The only reference was contained in *Schwarz*,[1258] where the Court minimized the risks involved by the use of biometrics. In particular, it declared that "taking two fingerprints "is not an operation of an intimate nature…nor does it cause any particular physical or mental discomfort" and that "The combination of two operations designed to identify persons may not *a priori* be regarded as giving rise in itself to a greater threat to the rights" in article 8 (grounds 48 and 49). In the SurPRISE project, sensitive data was proposed as a potential core of the right.[1259]

From the perspective of identifying attributes, sensitive data cannot constitute an autonomous attribute: to propose the opposite would defy the tenet whereby all personal data deserve protection irrespective of their sensitivity.[1260] Rather, sensitive data should be seen as a type of personal data that transversally affects all attributes, and calls for heightened safeguards or a lower threshold for interferences. In this respect, it could be seen as a specification of the rule of law (proportionality) enshrined in the test for permissible limitations: when the interference is potentially greater, the threshold of permissibility is reduced.

3.2 SUMMARY OF THE ATTRIBUTES OF ARTICLE 7 OF THE CHARTER

The table below summarizes the attributes of article 8 of the Charter. The first row on the left contains the attribute. The row beneath summarizes its content. The last row contains a summary of the essence. 'CJEU' precedes an essence was openly identified by the CJEU, whereas 'experimental' introduces suggestions for core areas that I have identified experimentally. Empty cells correspond to the absence of cores. The asterisk * identifies attributes likely to consist of a checklist.

[1258] *C-291/12 - Schwarz*.
[1259] See, in particular, Scheinin in Porcedda, Vermeulen and Scheinin (2013).
[1260] The point of sensitive data is to highlight the inefficiency of normally applicable law in ensuring adequate protection, which carries with it the possibility, but not the obligation, of a ban on processing. Simitis (1999), *Revisiting sensitive data*.

Attribute	Legitimate processing (attribute of the rule of law)*	Oversight*	i.supervisory authority*	ii.human intervention	Data subjects' rights	Minimization and accuracy	Security
Description	In sum, this attribute refers to the expectation for the data subject that the processing must be legitimate, which refers to three interconnected principles stemming from the rule of law: • Fairness and transparency • Purpose limitation (includes storage limitation) • Lawful legal basis	Oversight refers to the availability of oversight concerning data processing and the respect of the principles relating to the processing of personal data. It paves the way to two attributes.	This attribute, which stems from the rule of law, means that the individual can claim without hindrance the intervention of an authority for the protection of his or her right.	This attribute means that decisions significantly affecting an individual cannot be taken by a machine, and that a human being must be involved in the process	This attribute substantiates the notion of data subjects' control over their personal data, enabling them to intervene in the processing. It includes the following steps, which should be seen as a range of options available to the data subject depending on the situation: • Accessing the data and obtaining a copy • Rectifying inaccurate data • Objecting to processing, including profiling • Restricting the processing of one's personal data • Erasing data	This attribute has strong connections with purpose specification, data subjects' rights and security. It embodies an additional element of control of personal data, whereby individuals should communicate the minimum amount of personal data possible for a given purpose (data minimization) and that, within this category, the link between the information and the uniqueness of the individual should be maintained, in the guise of accurate and up-to-date data (accuracy). Hence, it has two sides to it • Data are adequate, relevant and non-excessive ○ Data are accurate and up-to-date	This attribute means that the individual can trust that personal information is protected against risks of a varying nature and likelihood which could effect physical, material and non-material damage
Essence – CJEU/ experimental	No			Experimental: the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision	Experimental: Access and objecting to profiling		CJEU: The provision of security safeguards in the legal basis relied upon for the
	Sensitive data: lowers the threshold of permissible interferences						

Table 19 Summary of attributes of the right to the protection of personal data

4 PERMISSIBLE LIMITATIONS OF ARTICLE 8 OF THE CHARTER

In section 1 I argued that article 8 should be construed in accordance with article 52(2) of the Charter. As a result, once appropriate rules for the processing of personal data pursuant to article 16 TFEU and 39 TEU will enter into force, the regime contained therein will represent a correct implementation of the right (until the Court will find the opposite). In an *obiter dictum* in *Schrems*, the ECJ stated:

> *"Measures of the EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality (judgment in Commission v Greece, C-475/01, EU:C:2004:585, paragraph 18 and the case-law cited)."*[1261]

Hence, such rules should also discipline the regime for permissible limitations, to which the right to the protection of personal data is subject,[1262] construed (narrowly like all exceptions[1263]) in the light of the Treaty and the Charter, and EU general principles of law. In practice, recital 73 of the General Data Protection Regulation (GDPR) states that restrictions on principles of personal data protection "should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms." It is important to note that the reference is to the ECHR as a whole, which does not challenge my proposal to interpret personal data protection primarily in the light of EU law since, as discussed in chapter 1, the ECHR is seen as an authority on the rule of law in general. The recital does not, instead, refer to article 8(2) ECHR which, in my view, confirms the independence of the right.[1264]

As seen *supra* (sections 1.1 and 1.5), this does not mean that article 8 ECHR becomes irrelevant, but rather that EU secondary rules should take precedence over conflicting interpretations of article 8 (1) and (2) ECHR if they offer higher levels of protection. The

---

[1261] *C-362/14 - Schrems*, para 52.

[1262] Similarly to the right to respect for private and family life, personal data protection is not absolute, but must be considered in relation to its function in society. *C-291/12 - Schwarz*, para 33; *C-543/09 - Deutsche Telekom*, para 51.

[1263] Since the provisions of data protection law must be interpreted in the light of the fundamental rights set out in the Charter, exceptions to those provisions must be narrowly construed. *C-212/13 - Ryneš*, para 29. Moreover, to ensure that the objective set in secondary law is attained, its provisions "cannot be interpreted restrictively", and they have "broad territorial scope", *C-131/12 - Google Spain and Google*, paras 53-54.

[1264] The EDPS states, instead, that the Charter has pre-eminence, but article 8(2) ECHR must also be taken into account. European Data Protection Supervisor, *Developing a 'Toolkit' for Assessing the Necessity of Measures that Interfere with Fundamental Rights* (Background Paper for Consultation, 2016).

rationale is to ensure the independence of Union law and its capability of offering greater protection than interpretations pursuant to article 8 ECHR. In practice, this means that article 8 ECHR would have a different relevance depending on the difference in scope of private life and data protection described by Kranenborg,[1265] as discussed *supra* (section 1.1). If the processing of personal data falls outside the scope of private life and within the scope of data protection, the case law of the ECtHR would not supply guidelines for the interpretation of article 8 of the Charter. If the processing of personal data is within the scope of private life and within the scope of data protection, within or outside the special regime for the protection of sensitive data, the relevant case law of the Strasbourg Court would supply guidelines of special significance.

Hence, permissible limitations will have to be defined on the basis of article 52(1) of the Charter and an autonomous test of the CJEU, for which the ECHR will supply guidelines having 'special significance', which, in my view, is what is happening when the CJEU refers to ECtHR case law 'by analogy'. In this respect, attention should be paid to the interpretation offered by the Article 29 Data Protection Working Party and the EDPS. [1266]

A case in point is *Digital Rights Ireland*. There, the ECJ avoided answering questions concerning the relevance of article 8 ECHR in the interpretation of article 8 of the Charter, thus leaving the matter open. However, as I noted in chapter six, *Digital Rights Ireland* marked a change *vis-à-vis* a case like *Österreichischer Rundfunk and Others*. Instead of analysing the matter through the lens of article 8(2) ECHR, the Court assessed the compatibility of Directive 24/2006/EC with the rights enshrined in article 8 (and 7) of the Charter pursuant to article 52(1) of the Charter, and referred to relevant cases of the ECtHR by analogy. This led to the development of a test for permissible limitations in the context of article 52(1) of the Charter. In chapter 6 I also noted that strict comparative research is needed to assess whether the approach chosen by the ECJ would lead, in practice, to a more protective outcome than the ECtHR in suitably comparable cases. Based on the discussion in section 1.2.2, the answer tilts towards the positive. However, here the form matters perhaps more than the content, in the sense that the existence of article 8 sanctions, in practice, the independence between the two human rights instruments (insofar as articles 7 and 8 are concerned), as confirmed by the Court in its opinion on the accession to the ECHR.

[1265] For him, "the interest of the data subject increases gradually." Kranenborg (2008), p. 1094.
[1266] Article 29 Data Protection Working Party (2014), *Opinion 01/2014, WP 211*; European Data Protection Supervisor (2016).

The test for permissible limitations elaborated in *Digital Rights Ireland* and presented in chapter 6 (section 4.2) could provide a specific adaptation of Scheinin's test discussed in chapter 5. In turn, the test for permissible limitations enriched by the core-periphery method is a necessary passage for the assessment of the impact of technologies on fundamental rights (step 4 of the methodology discussed in chapter 5, section 3.4; I discuss this in the next chapter).

As a conclusive point, I should restate the findings of the CJEU in *Dereci* (which concerns article 7 of the Charter) and *Bavarian Lager Ltd.* (appeal), where the Court said that article 8 ECHR is of relevance in situations that are not covered by EU law.[1267] Hence, the permissible limitations elaborated in the context of article 8 ECHR, and in Convention 108, should apply (to the extent that they do not raise exemptions themselves) to measures that fall outside the scope of EU law, notably national security (which is the exclusive competence of Member States). In the *Bavarian Lager Ltd.* appeal, the ECJ stated that

> *"It is clear from the first sentence of recital 15 of Regulation No 45/2001 that the Union legislature has pointed to the need to apply Article 6 EU and, by that means, Article 8 of the ECHR, '[w]here such processing is carried out by Community institutions or bodies in the exercise of activities falling outside the scope of this Regulation."*[1268]

It could also be argued that the protection and the regime for permissible limitations elaborated in the context of article 8 ECHR, and in Convention 108, could apply pending the adoption of legislation pursuant to article 39 TEU in the context of the CFSP. As anticipated in section 1.3, Convention 108 applies to national security and defence matters,[1269] subject to the conditions of article 9 of the Convention, which are modelled on the limitations to article 8 ECHR.[1270] Limitations must be provided for by the law of the Member State (principle of legality), and 'necessary for the protection of fundamental values in a democratic society' (in the light of the conditions of each signatory party), namely enforced for reasons of state security,[1271] public safety, monetary interest of the state, suppression of criminal offences,

---

[1267] Judgment in *C-256/11 - Dereci and others*, para 72. A contrario, "the applicability of EU law entails the applicability of the fundamental rights guaranteed by the Charter". *Joined Cases C-446/12 to C-449/12 - Willems*, para 49.

[1268] *C-28/08 P - Bavarian Lager Ltd.*, para 62.

[1269] And to the AFSJ, currently not covered by Directive 95/46. Article 29 Data Protection Working Party (2014), *Opinion 01/2014, WP 211*.

[1270] Explanatory Memorandum of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe.

[1271] As mentioned in the comment to article 9, "The notion of 'State security' should be understood in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State." Ibid.

protection of the data subject, or protection of the right and freedoms of others. In any case, the norms applicable in the CFSP should not be less protective than those identified in Convention 108, which identifies minimum safeguards (*supra*, section 1.3). Hence the personal information dimension of article 8 ECHR should be of relevance only when EU law does not apply.

***

Having derived the attributes for both privacy rights (step 3 of the method), it is now possible to try to establish a link between the technical and the legal understandings of the right, with a view to studying concrete technologies, as I set out to do in the next chapter.

CHAPTER 8 – AN INTERIM EPILOGUE

This chapter represents the last part of my enquiry before drawing the final conclusions. This journey aimed at defying the trade-off between security and privacy rights in general, and in cybersecurity in particular. Classic legal argumentation provided sound grounds against reliance on the trade-off; an in-depth scrutiny of the terms of comparison also showed it is a methodologically flaw intellectual device, as it provides a biased understanding of the terms of the equation. Once '(cyber)security' and 'privacy rights' are properly re-appraised, their relationship appears more nuanced, and is mediated by otherwise overlooked dimensions, chiefly technology. If this fatally wounded the over-simplistic trade-off model, and even opened up avenues for integration between security and privacy, on the other hand it raised new questions. Looked at from the perspective of applicable law, technology can play both a protective and an infringing role, which leads to the paradox of the same technology being both permissible and impermissible, leading to a seeming impasse.

In this second part of the thesis I have tried to factor in, or internalize, technological elements in legal analysis, to appraise whether cybersecurity and privacy rights can be reconciled. To this effect, I have developed a method to study the impact of technology used in the fight against cybercrime (simplified as the opposite of cybersecurity) on privacy rights. The purpose of this chapter is to demonstrate how the method works, with a view to provide an interim answer to the research question.

The methodology consists of five steps, which I recall in section 2. The first two steps were already completed in chapter 5 (sections 3.1. and 3.2), whereas chapter 6 and 7 developed the first two moves of step 3 (chapter 5, section 3.3), i.e. the identification of attributes and cores of both privacy rights. Step 3 involves one last move, i.e. 'linking attributes (and cores) to privacy canons' identified in step 2 (chapter 5, section 3.2), with particular reference to the technologies used.

The underlying idea is that, if we want to understand the interaction between cybersecurity and privacy rights, we need to understand the impact of cybersecurity-related technologies on the technical notion of information security and privacy (understood as protection goals), and link these to the legal understanding of privacy rights. As this move is a precondition for the further development of the method, I start with it in section 1.

Such an exercise bears significance for the second and third hypotheses of this thesis concerning reconciliation, whereby tackling narrow cybercrime/NIS would be complementary with maintaining privacy rights (hypothesis II) and pose no challenges in the investigatory phases (hypothesis III); broad cybercrime, by contrast, can be reconciled with privacy rights by implementing solid rule of law-oriented safeguards that abide by the notion of the essence and are mindful of the alternatives available.

In section 2 I recall the other steps of the method and illustrate how the proposed method can work in practice. To do so, I restrict the scope to narrow cybercrime/NIS, and justify my choice accordingly. The trial run of the method leads to deeper reflections on the research question, which I introduce by means of a discussion of the NIS Directive.

In the conclusion (section 3), I reason not only on the 'if' of reconciliation, but also on the 'how', with reference to the regulation of technology.

1. CROSSING CANONS WITH ATTRIBUTES

In chapter 5 I proposed exploring the theoretical link between, on the one hand, information and privacy protection goals, and on the other, the attributes of privacy rights. This is the third move of the proposed method (summarized *infra*, section 2), illustrated in the figure below.

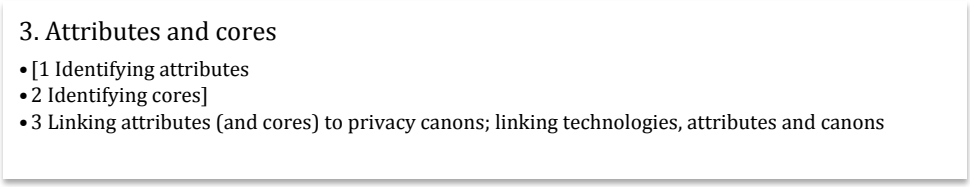


Figure 8 Diagram showing step 3 of the methodology

This third move is also an important precondition to assess the complementarity between privacy rights and NIS/ narrow cybercrime prevention, which, I recall, could mean overlap, convergence, or causality. It is also important in defining whether technologies respect,

protect and fulfil, or else infringe privacy rights, which has an important bearing on hypothesis 3 as to the possibility of reconciliation in relation to an investigation.

Table 20 reports the results achieved in chapter 5 (section 3.2), namely the relationship between the technical understanding of privacy and threats, as well as the overlap between privacy protection goals and information security goals. The first column to the left lists the privacy protection goals identified in chapter 5 (section 3.2.2), the second column provides their definition, and the third column to the left shows the threat associated with each protection goal (hence the name threat modelling).

Privacy protection goals	Definition	Threats
Unlinkability-Anonymity and Pseudonymity - Undetectability and unobservability	Privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context: processes have to be operated in such a way that the privacy-relevant data are unlinkable to any other set of privacy relevant data outside of the domain.	Linkability – Indentifiability - Detectability
Plausible deniability ✤	The ability to deny having performed an action that other parties can neither confirm nor contradict (e.g. a whistleblower can deny his or her actions)	Non-repudiation
Integrity* ❖	The property that data has not been altered or destroyed in an unauthorized manner.	Tampering
Confidentiality*	Hiding the data content or controlled release of data content	Disclosure of information
Availability* ❖	The property of being accessible and useable upon demand by an authorized entity.	Denial of Service
Transparency	Ensures that all privacy-relevant data processing, including the legal, technical and organisational setting, can be understood and reconstructed at any time. The information has to be available before, during and after the processing takes place.	Content unawareness - Policy and consent non-compliance
Intervenability	Intervention is possible concerning all ongoing or planned privacy-relevant data processing, in particular by those persons whose data are processed. The objective is the application of corrective measures and counterbalances, where necessary.	Non-intervenability
Information security only	**Definition**	**Threats**
Authentication	The process of corroborating an identity. 2. The provision of assurance of the claimed identity of an entity. 4. The corroboration of the identity of objects relevant to the establishment of an association. 5. The process of verifying the claimed identity of an entity to another entity. 6. The process intended to allow the system to check with certainty the identification of a party.	Spoofing
Authorization ❖	1. The granting of rights, which includes the granting of access based on access rights. 2. The granting of permission on the basis of authenticated identification. 3. The act of giving access to a service or device if one has the permission to gain access.	Elevation of privilege
Non-repudiation ✤	The ability to prevent a sender from denying later that he or she sent a message or performed an action.	Repudiation
Utility	The information is relevant and useful for the purpose for which it is needed	Arguably uselessness/ irrelevance

Table 20 Synthesis of threat modelling

This table ‘maps’ the relationship between the technical understanding of privacy and information security. The star symbol (*) indicates an overlap between privacy and information security protection goals: e.g. integrity is both a privacy protection goal and an information security protection goal. This leads to strong complementarity, i.e. overlap. Complementarity could also be achieved through authentication: while this is an information security goal, it is a specification of availability and integrity, and such interrelation is marked with the symbol ❖. The table also enables us to identify a case of a potential clash between privacy and information security protection goals, that of plausible deniability and non-repudiation (both are marked with the symbol ✜), which depends on the circumstances. The cross interactions of other protection goals require greater scrutiny.

The purpose of this section is to map the interactions between the technical understanding of privacy (and information security), and the legal understanding of the two rights. This is obtained by crossing protection goals with attributes. The two tables below show the correspondences between privacy protection goals and the attributes first for personal data protection (Table 21), and then for respect for private and family life (Table 22). The first column to the left lists the attributes of each right. The second column provides a synthetic explanation of the content of the attribute. The third column lists: cores relating to an attribute, if any; and when the core was found by the Court, which is marked at the beginning with the acronym ‘CJEU’. The fourth and last column lists the privacy protection goals, or canons, corresponding to each attribute.

Hence, by means of illustration, in the protection of personal data (Table 21), the attribute of Oversight by a supervisory authority (which is an attribute of the rule of law), whereby the individual can claim without hindrance the intervention of an authority for the protection of his or her right, is linked to two protection goals. The first one, which pertains to privacy only, is intervenability, i.e. the possibility to apply corrective measures and counterbalances where necessary. The second one is non-repudiation, which pertains to information security (and is at odds with plausible deniability), which means the ability to prevent a sender from denying later that he or she sent a message or performed an action, so that liability can be attributed.

Attributes of art. 8	Content	Core	Canons
Legitimate processing (attribute of the rule of law)*	The expectation for the data subject that the processing must be legitimate, which refers to three interconnected principles stemming from the rule of law: • Fairness and transparency • Purpose limitation (& storage limitation) • Lawful legal basis		Confidentiality Unlinkability Transparency (fairness and transparency) Authorization
Oversight*	Oversight refers to the availability of oversight concerning data processing and the respect of the principles relating to the processing of personal data. It paves the way to two attributes.		Intervenability Non-repudiation
i. Supervisory authority*	The individual can claim without hindrance the intervention of an authority for the protection of his or her right.		"
ii. Human intervention	Decisions significantly affecting an individual cannot be taken by a machine, and that a human being must be involved in the process	Experimental: the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision	"
Data subjects' rights	Data subjects' control over their personal data, enabling them to intervene in the processing. It includes the following steps, which should be seen as a range of options available to the data subject depending on the situation: • Accessing the data and obtaining a copy • Rectifying inaccurate data • Objecting to processing, including profiling • Restricting the processing of one's personal data • Erasing data	Experimental: Access and objecting to profiling	Integrity Availability Transparency Authentication Unlinkability (profiling) Non-repudiation
Minimization and accuracy	Individuals should be enabled to communicate the minimum amount of personal data possible for a given purpose (data minimization) and that, within this category, the link between the information and the uniqueness of the individual should be maintained, in the guise of accurate and up-to-date data (accuracy). Hence, it has two sides to it: • Data are adequate, relevant and non-excessive • Data are accurate and up-to-date		Integrity Unlinkability (for minimization) Utility
Security	The individual can trust that personal information is protected against risks of a varying nature and likelihood, which could effect physical, material and non-material damage	CJEU: The provision of security safeguards in the legal basis relied upon for the processing of personal data	Confidentiality Availability, Authentication and non-repudiation (organizational measures) Intervenability
Sensitive data: lowers the threshold of permissible interferences			Unlinkability, confidentiality [Plausible deniability]

Table 21 Relationship between information security canons, privacy canons, and attributes of article 8

As for private life (Table 22), the attribute of communications concerns the ability to share information with other individuals, under the presumption that information shared privately should remain confidential, regardless of its content and the mode of communication, and with the expectation that information shared privately will not be used against the individual. The content of communications represents, for the CJEU, an element of essence. A number of protection goals correspond to this attribute, which is of central importance for information security. First, and not so obviously, Authentication/authorization, in the sense of allowing the system to check with certainty the identification of a party (the intended sender or recipient of communications), and subsequently gaining access to a service or device if one has the permission to access it. Second, and obviously, confidentiality, which possibly carries with it the desirability of plausible deniability, for instance in the case of a whistle-blower wishing to deny her or his actions. Note, as anticipated in chapter 5 (section 3.2.3), that while non-repudiation can be fundamental for personal data protection, it can be problematic for confidential communications. This bears very interesting reflections, such as the fact that technology fosters complementarity, but it also exposes elements of tension (but not a trade-off!); there can be a clash between personal data protection and private life, as hypothesized in chapter 2, which testifies to their independence. Clashes may also appear within a right: plausible deniability may be very important to protect the meta-attribute of sensitive data, and hence exercise other rights freely.

Attributes of art. 7	Content	Core	Canons
Private life	Those elements that are relevant to develop and maintain one's personality and identity, understood as unique and worthy of equal respect.	See sub-attributes	Utility
i. Physical and psychological integrity	• The *forum internum* of the mind, i.e. one's thoughts, feelings and emotions. • The *forum internum* of the body: genetic characteristics and unique physical traits • The *forum externum* of the body: the right to own one's body and protect it from undesired or forced access to it.	The *forum internum* of the mind and of the body	
ii. Personal social and sexual identity	The '*forum externum*' of mental integrity, which is substantiated in the coherent portrayal of one's personality and identity to the external world. It includes control over one's name, the upkeep of one's reputation, the expression of one's sexual orientation, but also the manifestation of one's beliefs and personality in the form of attitudes, behaviours and clothing.	The expression of one's sexual identity (CJEU) Official recognition of one's original or acquired name; Faithful social representation of one's identity	
iii. Personal development, autonomy and participation ('outer circle')	The partaking of individuals in the democratic society • The development of one's personality in the spirit of self-determination • Autonomy of one's movements and actions • Participation in the social and political life as one sees fit All the above require a minimum degree of control, even if conducted in public. The possibility to develop social relations of an amicable or professional nature. In this sense, this sub-attribute concerns the 'outer circle' of one's life and links with the 'inner circle' of one's family.	Absence of secret external constraints	
Family	The 'inner circle', one's kin by blood and election, which represents the first mode of existence in society and comes before the state. It includes horizontal and vertical relationships regardless of their seal of legitimacy, and substantiates in emotional and material ties with individuals and surroundings.	For a father, the possibility to apply for the right to custody (CJEU) Continuity of relationship of care; Recognition of relationship of care	
Communications	The ability of individuals to choose with whom and how to share information, and the presumption that information shared privately should remain confidential, regardless of its content and the mode of communication. This includes the expectation that information shared privately will not be used against the individual.	The content of one's communications (CJEU)	Confidentiality [Plausible deniability] Authentication/ authorization
Home	One's settled and secure place in the community, where individuals can develop ties of an intimate nature and nurture self-determination, far away from the public gaze and undesired intrusion.	A minimum zone of physical intimacy	[Unlinkability confidentiality]

Table 22 Relationship between information security and privacy canons and attributes of article 7

Crossing information security canons, (technological) privacy canons and (legal) privacy attributes unveils a convergence between protecting privacy rights and NIS and combatting narrow cybercrime that goes beyond legal provisions or judgments (as discussed in chapter 4). To be sure, it has to be kept in mind that the identification of canons and attributes is preliminary and must stand the test of peer review. Yet, this seems to offer a promising element in the direction of validating the second hypothesis, on complementarity (overlap/convergence), and sheds light on causation (whereby 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, or vice versa).

In this spirit, the illustration of the method, which is the focus of the next section, focuses on NIS/narrow cybercrimes.

2. TESTING THE METHOD

The diagram below illustrates the five steps of the methodology elaborated in chapter 5. I recall the meaning of each step of the method in the corresponding sub-section (section 2.1 is step 1, section 2.2 is step 2 etc.).

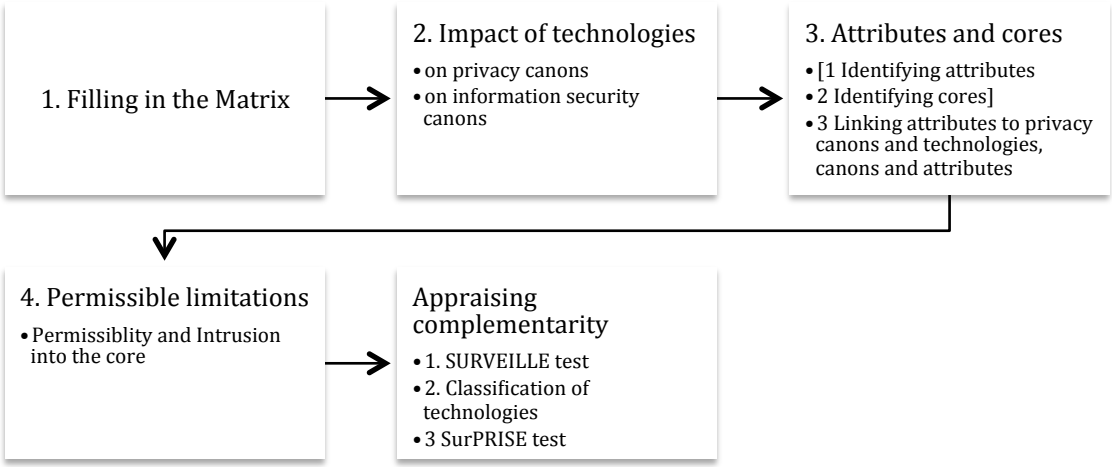


Figure 9 Diagram showing the 5 steps of the methodology

2.1 EXAMPLE OF MATRIX FOR DATA INTERFERENCE

The first step consists in building a matrix linking the legal and technical understandings of a given cybercrime. Since the purpose of this exercise is to illustrate how the method would work, the choice of the offence to test it with is not irrelevant.

An immediate choice would seem that of illegal interception, which refers to data disclosure as well as elevation of privilege, and thus negates confidentiality and authentication, which in turn is connected to the security attribute of article 8 of the Charter, and the confidentiality attribute of article 7 of the Charter, both of which have been identified as expressing core elements of the rights by the CJEU. Often interception is done at the physical level, and detection and analysis consequently require physical inspection.[1272] Prevention is a better option, the classic instrument being encryption, which responds to both privacy and information security canons, and enables preserving the core of both rights as identified by the Court. Such an overlap is very likely to validate hypothesis 2 (though the method should still be run through). However, this is neither a great surprise, nor does it prove conclusive for the other types of narrow cybercrime. Hence, it represents a typical example of a 'smoking-gun test', which confirms the hypothesis but does not eliminate others.[1273] This, however, pushes for a different test. I will come back to illegal interception in section 3.

Here I prefer focussing on illegal data interference which, pursuant to article 5 of Dir. 2013/40 on attacks against information systems, means "deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and without right," and "is punishable as a criminal offence, at least for cases which are not minor".

There are multiple reasons for choosing this offence: it is an offence that has immediate relevance for personal data protection (and communications), due to the importance of integrity for both cybersecurity and privacy rights; it creates a link with the case study in chapter 4 and allows looking again into deep packet inspection; and technical solutions are widely available for all steps. Hence it appears to be a case with greater relevance. It should

[1272] Georg T. Becker and others, 'Stealthy Dopant-Level Hardware Trojans' in Guido Bertoni and Jean-Sébastien Coron (eds), *Cryptographic Hardware and Embedded Systems - CHES 2013* (Springer 2013); Landau (2010), *Surveillance or Security?*

[1273] David Collier, 'Understanding Process Tracing' (2011) 44 Political Science and Politics. Collier (p. 825) recalls "the usual caveat that the definitive elimination of a hypothesis is often hard to achieve in social science."

be remembered that, when it comes to crimes against CIAs, real-life cases may involve committing several offences at a time. For instance, the placing of malware for the sake of tampering with data typically entails the use of specifically designed tools (art. 7 of the Dir. 40/2013) and illegal access, and can lead to illegal interception.

Going back to the methodology, the first step consists in drawing a matrix that relates the legal understanding of the offence to the technologies used to perpetrate, prevent/detect-mitigate or detect-investigate the offence, and the 'block' of cyberspace in which such offence takes place (meaning either the element of cyberspace concerned, or the layer of the Internet).

Tech/tool	Substantive issues			Tools used to		
Illegal data interference	**i) Definition/ legal basis**	**ii) Corresponding threats/behaviour**	**iii) The affected block of cyber-domain**	**Perpetrate**	**Prevent/detect-mitigate**	**Detect-Investigate**
Dir. 2013/40/EU, art. 5; **Dir. 2001/29/EC, art 7**	Deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor	Worms, viruses, malware, tampering, defacing	Various	Malware	Intrusion detection systems (Firewall/ Anti-malware/ update software/ machine learning/ packet inspection	Sandbox/ honeypots / anti-malware/ DPI
			Network level	Malware (e.g. Conficker)	SUSTOR	DPI/DCI E.g. LAN Guardian
			Device level	Web-based malicious ad-injection/ Cross-scripting	Keeping one's software updated	Intrusion Detection System/ Firewall
			Document level	PDF tampering /malware	Trust services e.g. e-signatures and time-stamping	Anti-virus software/ forensic

Table 23 Example of matrix in case of illegal data interference

The threats corresponding to this offence are worms, viruses, malware, tampering and defacing (see chapter 3, section 3), which can act at different layers of the Internet. These are prevented, in the sense of blocked, by intrusion detection systems (firewalls) and anti-malware based on packet inspection and machine learning, as well as keeping one's software updated; attempts at illegal data interference can be investigated by means of sandbox, honeypots, deep-packet inspection and anti-malware with such functions. The table provides some illustrative examples. The second row from the top shows examples of data interference at network level that can be detected by means of intrusion detection systems such as SUSTOR and LanGuardian, and investigated with the latter. The row immediately underneath provides an example of data interference at the application level, whereby advertising icons lead to malware that can attack one's system if it finds vulnerabilities. Apart from not clicking on the ad, keeping one's software updated is a way to prevent this from happening. The third example, in the fourth row from the top, consists in tampering at the document level, with PDF-specific malware inserted through obfuscation techniques in PDF documents, which can be prevented by using anti-tampering trust services and detected with appropriate software.

In the following I focus on the off-the-shelf DPI software LanGuardian.

2.2 Analysis of tools: Description of LanGuardian (detection and analysis)

Let us take the case of generic malware, which is malicious software that violates a security policy without self-propagating. *Prima facie*, this is a situation of illegal data interference, which corresponds to tampering, i.e. the altering or destroying of data in an unauthorized manner. It affects the attribute of accuracy (minimization) and consequently the data subject's rights of rectifying one's data. Since tampering entails a violation of authorization, it also violates the legitimate processing attribute.[1274]

NetFort LanGuardian[1275] is a self-sustaining DPI software for network management, including virtual networks, that does not require 'bespoke hardware' (as it runs on industry

[1274] In a complete test of the method, a specific example of malware would be taken into account, and its impact on protection goals and attributes would also be assessed.
[1275] Deep-packet inspection tool: https://www.netfort.com/languardian/ retrieved from WikiLeaks, 'DotForce Newsletter - Giugno' (*Hacking Team*, 2015) <https://wikileaks.org/hackingteam/emails/emailid/92171>.

standard PCs and servers[1276]) or installing any other software. The vendor presents it as a "full packet capture product",[1277] and proposes its use for a host of different functions: monitoring user activity, files, web network and Virtual/Mobile environments; bandwidth troubleshooting; wire data analysis; network forensics; packet capture; Windows file share; security information and event management (SIEM) and log Management (streaming a subset of the network traffic data in standard syslog format); and data compliance. Here I limit myself to studying what concerns illegal data interference: "file activity monitoring" and "detecting source[s] of malware such as Conficker" [1278] or "tracking Ransomware".[1279]

It is worth stressing that the following analysis is illustrative, in that it cannot benefit from an in-depth understanding of data flow diagrams, which would require cooperation with a computer scientist (chapter 5, section 3.2; see also *infra*, section 3). Rather, the analysis of the technology rests on the vendor's description.[1280]

According to NetFort, LanGuardian analyses network traffic based on the Microsoft Server Message Block (SMB) protocol. This is a network file-sharing protocol, which enables sharing between clients and servers, and is used on third-party products such as OpenVMS, HP-UX, Solaris, Novell Netware and Linux and Samba (the open source implementation). LanGuardian is advertised as a scalable product that can be used anywhere from a single office to a global corporate network.

LanGuardian includes several engines, which support: a network intrusion detection system (IDS) working in real time; the creation of an Active Directory of users by IP or MAC address, and even username (when integrated with Microsoft Windows); and real time, user-specific application traffic analysis on internal network activity, e.g. access to intranet servers and file shares, or external activity such as access to websites, cloud services and social media.

LanGuardian connects to a mirror port (e.g. SPAN port, TAPs) and extracts the user wire data (raw data) from network packets (or packet analyser solutions like Wireshark), and logs user activity (traffic data) for months or even years. The collected information is indexed and

[1276] NetFort, *Unified Network Traffic Monitoring for Physical and VMWare Environments* (White Paper, 2010), p. 9.
[1277] Ibid.
[1278] Dan Goodin, 'Police Body Cams Found Pre-installed with Notorious Conficker Worm' *ArsTechnica.com* (16 November 2015). For a more technical overview, see the TrendMicro Threat Encyclopedia, at: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/conficker (last access 16 December 2016).
[1279] See at: https://www.netfort.com/languardian/.
[1280] NetFort (2010). And the various pages of the vendor's website: https://www.netfort.com/languardian/.

stored on a traffic database capable of producing historical activity reports as well as trends for studying one's network; it can be accessed via the "browser-based user interface". The system does not block users or deny them access, but simply communicates with the network manager.

Wire data is described as data contained within the headers and payloads of network packets moving from one node to the other. LanGuardian enables analysis to be performed on such data by "converting raw packet data into human readable format" so as to observe information such as start-time, end-time and size of individual data transfers, IP of source and destination, the protocol, file names, URIs, and Type of Service (TOS). NetFort argues that such capture "does not require auditing on servers so will not slow down business critical applications". [1281]

According to NetFort, LanGuardian offers compliance with applicable law because, among other things, it enforces segregation of duties and enables checking on sensitive data. Despite having a base in Ireland, the EU legal framework is not mentioned. Hence, it is time to look into the impact on security and privacy canons.

***

Regarding information security canons, LanGuardian seems to have a positive impact on integrity and availability, and potentially on authentication. On the other hand, it has a potentially negative impact on confidentiality (from the perspective of users), non-repudiation (concerning the claim that data capture "does not require auditing on servers") and utility, in that it may access excessive information for the objective pursued.

On top of confidentiality, LanGuardian has a direct impact on unlinkability, in that it links privacy-relevant data across domains, it enables identifying users and detecting them, and transparency, because nowhere can it be inferred that users are warned of these activities. If logs are not kept, it may lead to plausible deniability, which, in this case, plays against the needs of the user.

Hence, LanGuardian seems to have a mixed impact, positive and negative at once, on both network and information security and privacy rights.

[1281] See at: https://www.netfort.com/languardian/.

2.3 STEP 3 AND 4: CROSS-IMPACT ON ATTRIBUTES AND TEST FOR PERMISSIBLE LIMITATIONS

In practical terms, steps 3 and 4 should be integrated, in that the relationship between privacy canons and attributes serves a test for permissible limitations, and attributes serves the identification of cores.

LanGuardian is offered to network administrators of private networks, and therefore they would not fall within the remit of the Framework Directive, the e-Privacy Directive nor the Open Internet Access Directive (discussed in chapter 4). Yet, it should be noted that these frameworks can be relevant for determining principles of conduct by analogy, since they concern the same 'block' of cyberspace, i.e. networks. If network administrators using LanGuardian represent essential services or digital service providers, they can fall within the remit of the NIS Directive[1282] – it should be recalled that BEREC left the door ajar for subsuming corporate networks under the remit of the Open Internet Access Directive (chapter 4). In their activities as data controllers (or processors), they would be liable to the rules of the Data Protection Directive, and the GDPR in the future.

Given this framework, a legal basis enabling the use of this system could be found in articles 14(1) and 16 (1) of the NIS Directive, which similarly oblige Member States to ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems. Article 16(1) could be particularly suitable as a legal basis, in that digital services using network and information systems to offer their services should take into account the following measures "(a) the security of systems and facilities; (b) incident handling; (c) business continuity management; (d) monitoring, auditing and testing; (e) compliance with international standards." Letters (a), (c) and (d) seem good candidates to provide a legal basis.

In the test for permissible limitations, it is not sufficient that there be a law, but that such a law is of sufficient quality and provides the necessary safeguards. Truly, a weak spot of such a legal basis could be the absence of suitable guarantees, as was the case for the Data Retention Directive in *Digital Rights Ireland* (note the common legal basis, art. 114 TFEU and former art. 95 TEC). In this respect, it is legitimate to ask why providers of essential

[1282] Note that the permissibility of monitoring in the workplace is outside the scope of this illustrative discussion. Likewise, the potential use of LanGuardian in academic contexts (as the vendor seems to advertise) will feature in subsequent developments of this work.

services, or digital service providers, have not been explicitly constrained by the same principles applicable to ISPs and Telecommunications Companies (Framework, e-Privacy and Open Internet Access Directives) which, in protecting their networks, should neither enforce general monitoring, nor intrude into the content of communications (the two being two sides of the same coin), unless strict safeguards apply. This may be simply clarified in court – or Member States may have learnt the lesson of the Data Retention Directive and provide the necessary guarantees in national law (which could simply consist in an amendment of existing Telecom legislation), so that the chances of the CJEU expressing itself over the NIS Directive would be sensibly reduced.

Let us set aside the suitable safeguards in law, because the second step of the test for permissible limitations concerns respect of the 'essence' of the right. It is actually at this stage that the added value of the proposed methodology should become apparent. How to appraise whether the 'technical measure' used respects the essence? The technology used needs to be looked into.

Clearly the violation of confidentiality, particularly for what concerns the payload, seems to call into question both the core of personal data protection and the respect for private life, a situation that was tackled by the CJEU, under different premises, in *Scarlet*, *Sabam* (C-360/10) and *Digital Rights Ireland*, and that I have discussed in chapter 4 (section 2.4). There, I discussed the ambiguity of the "acquisition of knowledge of the content of the electronic communications"; as the content of the message may not be physically read, that could prove a subtle line for the admissibility of the method *vis-à-vis* its seeming usefulness to tackle integrity and availability. The violation of unlinkability could encroach upon another (experimental) core of the attribute of individual rights, namely resistance to profiling. Two violations of information security canons, non-repudiation and utility, can also have a bearing on other cores. As for non-repudiation, individuals may not be able to receive oversight in the form of human intervention, and instead be made the object of automated individual decisions; as for utility, the expression of one's sexual life, which forms a recognized core of private life, could also be compromised.

Moreover, the fact that LanGuardian seems to be accessible via a browser may expose data to loss of authorization and eventually confidentiality, in a way that could cause a major incident both for security and for privacy rights.

Hence, LanGuardian may not pass the test for permissible limitations on grounds of disrespect of the essence of privacy rights (and NIS may be struck down for lack of suitable safeguards).

2.4 OVERALL ASSESSMENT

The SURVEILLE and SurPRISE methods aim at comparing different tools; given the limited number of tools revised, assessing complementarity at this stage may be misleading.

Prima facie, the LanGuardian may not pass the test because of its potential encroachment on the court-sanctioned core of the attribute 'confidentiality of communications', namely content (right to private and family life), but also the experimental core of the attribute 'individual rights', i.e. resistance to profiling (right to the protection of personal data). Given the lack of transparency of the tool, particularly the absence of logs, another potentially encroached core is 'oversight in the form of human intervention', of the attribute automated individual decisions (right to the protection of personal data). LanGuardian could be seen to be an impermissible PIT, which violates these rights.

The analysis of this technology appears to conform to a "straw in the wind" test[1283] *vis-à-vis* hypotheses II and III, i.e. it slightly weakens them without eliminating them. It weakens hypothesis II because, as a preventive-detective technique, complementarity is achieved by encroaching on the essence of the rights, and hypothesis III, because as an investigative technique, it is not privacy rights agnostic, but rather encroaches on them, as in the case of broad cybercrimes. But does this mean there is no reconciliation? Certainly not, since this example was only illustrative of the way how the method could work, and *supra*, section 2.1, I hinted at encryption as a likely "smoking-gun test". Moreover, one of the outcomes of SURVEILLE was that a seemingly impermissible technology could become permissible if used pursuant to an instrument compliant with the rule of law, and with the implementation of privacy by design. With reference to LanGuardian, the application of PbD may lead to a different result. Following BEREC recommendations, "the actual traffic management measure preserving integrity and security is triggered only when concrete security threats are

[1283] Collier (2011).

detected."[1284] This could be the case with profiling infringing users. Such form of monitoring should be subject to strict auditing so that, instead, it does not lead to other forms of traffic management or an unlawful monitoring of usage.

BEREC also recognizes that, "in order to identify attacks and activate security measures, the use of security monitoring systems … is often justified. In such cases, the monitoring of traffic to detect security threats…may be implemented in the background on a continuous basis".[1285] Such monitoring should be subject to strict interpretation and to proportionality requirements, and closely assessed by National Regulatory Authorities. In other words, as anticipated in chapter 4 (section 2.3.), the potential interference should be adequate, i.e. it should be appropriate to achieve the intended objective and be the least intrusive among a range of available measures. This raises questions about the notion of interference with the essence of fundamental rights, which I will deal with in the conclusion.

Hence, the permissibility depends on the technology chosen because of how it is designed, i.e. on the functions that are implemented. In other words, reconciliation can be achieved, but as the result of an explicit choice. This leads to a final reflection: if the law is silent about such objectives, how can reconciliation be achieved, in practice? This sheds new light on the second part of the research question, i.e. how can there be reconciliation between cybersecurity and privacy rights.

2.4.1 The NIS Directive would fail the Digital rights Ireland test, and enable sleep-walking into fundamental rights violations

Earlier I reasoned on the guidelines of BEREC on the open access Directive, but as I noted in section 2.3, LanGuardian users may fall outside the scope of the Directive. They may, instead, fall within the remit of the NIS Directive, particularly its chapter IV and V on "security of the network and information systems" (arts. 14-18). As for essential services, which include Internet Exchange Providers (IXPs), domain name system service providers and Top Level domain name registries, the Directive is silent about monitoring. Monitoring is explicitly mentioned in article 16, which refers to digital service providers, i.e. online

[1284] Body of European Regulators for Electronic Communications (BEREC) (2016), *Guidelines on net neutrality, BoR (16) 127*, para 85.
[1285] Ibid.

marketplace, online search engines and cloud computing services, among the elements to be taken into account within 'technical and organizational' measures to manage the risks posed to the security of network and information systems which they use. Such elements are to be specified by Commission implementing acts (article 16 (8)), which, in line with recital 69, should take into account "monitoring and logging policies, exercise contingency plans, network and information systems testing, security assessments and compliance monitoring." Article 2 of the NIS Directive lays down that the processing of personal data must be compliant with Dir. 95/46, which, it should be stressed, does not contain provisions on monitoring, as those are dealt with in the *lex specialis*, the e-Privacy Directive. However, the e-Privacy Directive would not apply to the addressees of the NIS Directive (perhaps the case could be made for IXPs, but this is outside the scope of the current discussion).

This begs the question as to whether it is appropriate for essential and digital service providers to be bound by no, or potentially lesser, standards than ISPs or electronic communications service providers. Indeed, this state of affairs may be prohibited. In section 2.3 above I noted that the NIS directive could meet the same fate of the Data Retention Directive.

To demonstrate it, I will briefly implement, as follows, an ideal 'test' of how the CJEU could assess the NIS Directive based on *Digital Rights Ireland*, mindful of the obvious differences between the cases. First, monitoring pursuant to the NIS Directive would likely interfere with articles 7 and 8 of the Charter (and 11[1286]), because the systems under analysis concern elements of private life, may affect the way in which users access and use means of communications, and constitute the processing of personal data. The Court would thus find the existence of a wide-ranging interference (§ 31-37), which could engender a feeling of constant surveillance (§ 37), and therefore apply a proportionality test based on article 52 of the Charter (§ 38-71). The Court may then find that the fact that the interference is wide-ranging does not impinge on the essence of the right (§37-40), possibly because knowledge of the content of the communication cannot be obtained, and that the NIS Directive meets an important objective of public interest in the EU (it aims support their fights against serious crime, § 24). The CJEU may eschew a technical analysis and find monitoring adequate, even with evidence that alternative and less invasive methods exist. However, the Court might alternatively find that, if modern techniques are instrumental to pursue public security,

[1286] Though it deems it unnecessary to assess the Directive in the light of article 11 of the Charter (§ 70).

however fundamental that objective is, it is not enough to establish the necessity of 'monitoring' (§ 51). The protection of rights requires having in place legislation that respects certain parameters of quality, to enable legal certainty (§ 54-55). On these grounds, the Court may find the Directive excessive on three broad grounds: first, the monitoring is all-encompassing, applies to all users of those services, without any specific restrictions; second, there are no rules disciplining the access, authorization and further use of data monitored (§ 60-62); third, monitoring applies evenly, without any criterion. On those grounds, the Directive would be disproportionate (§ 65).

The absence of specific safeguards would not only fail the NIS Directive on the proportionality test, insofar as monitoring is concerned. It also leaves the market free to find sub-standard solutions that silently violate fundamental rights. And this can have a bearing on the reconcilability of cybersecurity with privacy rights, or otherwise a reality where the two are artificially opposed, and pulled to the whims of different communities (whose interests may converge to the detriment of the individual and her privacy rights).

3. Concluding remarks: the need for technology mindfulness

This chapter provided a trial run of the methodology that I devised in chapter 5 and developed throughout part 2 of the thesis. The outcome of the analysis, which must be considered experimental, did not provide final answers to my initial hypotheses. This begs the question of which model of reconciliation (if any) is more likely. I tackle the likelihood of models of reconciliation, and additional reflections on the 'how' question, more widely in the final conclusions.

The reflections on the NIS Directive unveil a buried side of the 'how' question, which concerns the legislator's willingness to regulate technology, and the values it should pursue when doing so.

The "permanent revolution" embodied by new technologies forces us to face the so-called 'Collingrdige dilemma', which refers to the insight that "the potential benefits of a new technology are widely accepted before enough is known about future consequences or potential risks to regulate the technology from the outset, while by the time enough is known about the consequences and possible harms to enable regulating it, vested interests in the success of the technology are so entrenched that any regulatory effort will be expensive, dramatic and resisted."[1287]

If it is accepted that technology is never neutral, because of its ability to enable, or else inhibit, behaviour,[1288] then it should also be possible to argue that choosing technology neutrality (chapter 5, section 1) reinforces the Collingrdige dilemma. Technology neutrality may foster the unintended regulation of behaviour, as well as intentional techno-regulation by actors expressing strong vested interests, who lobby for the "crimification"[1289] of undesired conduct in cyberspace to suit their own needs.

Leenes defines 'Techno-regulation' as the "deliberate employment of technology to regulate human behaviour."[1290] To be sure, techno-regulation is not inherently bad: apart from making the commission of crime more difficult, it can protect individual's prerogatives, as in the case of PETs, or even enforce rights, as in the case of PbD.

Let us reflect on the case of PETs. Earlier In section 2 I anticipated that in the case of illegal interception, the implementation of requirements from data protection legislation seems *prima facie* to fully converge with those of network and information security, which both point to cryptography. Here there are two reflections. First, encryption does not hide everything: traffic data is left exposed. To use a visual metaphor, it is a bit like walking with a *niqab* in the city centre of Florence: no one can tell who you are, but you do attract everyone's attention (particularly of security forces), and everyone can see your trajectory, i.e. where you go from and to. Secondly, and as discussed in chapter 5 (section 3.5), Clarke defines encryption as savage PETs, which entails a certain lack of regard, both toward others, and in one's own approach to cyberspace.

[1287] Morag Goodwin, 'Chapter 1. Introduction. A Dimensions Approach to Technology Regulation' in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes (eds), *Dimensions of Technology Regulation* (Wolf Legal Publishers (WLP) 2010), p. 2, footnote 1.
[1288] Leenes (2011).
[1289] Adams and others (2015).
[1290] Leenes (2011), p. 149.

What is this to say? In the case of savage PETs, this means that even solutions that foster complete integration between the two objectives under analysis – cybersecurity and privacy – embody hidden values and downsides. The more general conclusion is that techno-regulation, i.e. regulating human conduct by means of technology, cannot be left to chance: it is the job of law and politics to re-appropriate decision-making as to which values technology should pursue. There are two sides to this. On the one hand, it means asking upfront what kind of goals regulations should achieve, thus making a conscious selection of the regulatory tool chosen, which may entail selecting technology-specificity over technology neutrality (chapter 5, section 1). On the other hand, it means that the discussion as to the goals of technology and the value it is meant to pursue should be transparent and accountable. As Brownsword put it, "a fully techno-regulated community is no longer an operative moral community."[1291] Brownword's words recall Julie Cohen's idea of a modulated democracy, discussed in chapter 2 (section 3.3.4), i.e. the creation of surveillance infrastructures that organize the world for us, force us to look at the world through their lens, and are ultimately exploited by powerful commercial and political interests.

Techno-regulation impacts on the *voulouir vivre* of a nation discussed in chapter 1 and 2, and ultimately the *ordre public* of societies. In other words, the question as to 'how' cybersecurity and privacy can be reconciled through technology matters as much as 'if' they can be reconciled.

[1291] Brownsowrd, R, "Code, Control and Choice: Why East is East and West is West" (2005) (25)(1) Legal Studies 1, 14, quoted in ibid, p. 159.

CONCLUSIONS

"And the end of all our exploring
Will be to arrive where we started
And know the place for the first time."
Thomas Stearns Eliot [1292]

1 SUMMARY OF FINDINGS

This journey started with the question "Can the rights to respect for private and family life and the protection of personal data be reconciled with the pursuit of cyber-security, as defined in the European Union? If so, how [can they be reconciled], taking into consideration technological constraints?"

In other words, I asked both an 'if' and a 'how' question. In relation to the 'if question', I advanced the hypotheses that: the trade-off model is not a useful intellectual device (I); that privacy rights are complementary with cybersecurity understood as NIS/narrow cybercrime (II); and that reconciliation can also be achieved in the case of broad cybercrimes (III).

As to the 'how' question, which concerns the mode of reconciliation, I advanced the following hypotheses: complementarity in the case of narrow cybercrime/NIS may be in the form of overlap (strong), causality (intermediate) or convergence (IIa, IIb, IIc); reconciliation could mean that the measures necessary for an investigation are privacy agnostic (IIIa), e.g. in the case of narrow cybercrime/NIS, *or*, in the case of broad cybercrime, the trade-off could be avoided with the application of instruments featuring solid safeguards (IIIb). According to a final hypothesis relating to the 'how' question and tied to the reference to technology, hypotheses II-III cannot be fully demonstrated by means of a classic legal analysis, due to technology neutrality, courts seeming deference to society on technology, and the open-ended understanding of privacy rights (IV).

The question as to whether the pursuit of cybersecurity can be reconciled with the protection of personal data and respect for private and family life is a specific instance of the trade-off between security and 'privacy rights', a debate sadly revived both by the terrorist attacks of 2015-2016, and Snowden's revelations of mass surveillance.

[1292] Thomas Stearns Eliot, 'Little Gidding' in Thomas Stearns Eliot (ed), *Four Quartets* (Harcourt 1943).

My first step in answering the question was therefore to argue against the trade-off model, using as a reference point Posner and Vermeule's elaboration of the trade-off and deference theses (chapter 1). I first clarified my normative assumption, namely that trading-off rights – any rights – with security should be rejected in the European Union, based on four interconnected grounds. Trading security and liberties as scarce resources (in this case, values), would be against the European Union's ideal *ordre public* (public policy), or its *vouloir vivre* (i), which is solidly anchored in the rule of law as an antidote against the tragic experiences of dysfunctional government that led to the catastrophe of WWII (ii). Such a backdrop informed the constitutional architecture of the Union, which features constraints against reducing civil liberties, also in the AFSJ (iii); at times of emergencies (iv), the constrained architecture of the Union relies on a multilevel system of protection featuring, underneath, Member States' courts, and above, the ECtHR. In addition to these normative arguments, SurPRISE project-related research also challenged the assumption that citizens desire to trade-off liberty for security.

Having set the normative ground, which concerns prescription, i.e. what *ought* to be, I moved onto the cognate hypothesis that the trade-off model is not an appropriate intellectual device (chapter 2). Hypothesis I built on the inconsistency of the factual claims of Posner and Vermeule's model, and consisted of three interrelated challenges to the model. The first challenge consisted in reappraising the terms of the equation 'security v. privacy'. I rebutted the unfortunate foundations of balancing, by expounding the value of the terms and the importance of 'privacy rights' in relation to the *ordre public* of the contemporary EU. I argued that security is a malleable concept, which is reflected in the EU legal system, where in any case it does not bear any independent legal value. Noting that 'security' is the expression of the absence of threats codified in offences, I added legal-descriptive meaning by arguing that any reference to security in a given discussion of the 'trade-off' must be replaced by the specific offence under analysis. I subsequently considered privacy, whose value as a moral and legal entitlement is overlooked. I recalled that in the Union legal order, privacy contains a double reference, that of two qualified rights, which must be kept separate: private and family life, and the protection of personal data. In contrast to security, I argued that privacy requires the addition of a legal-normative meaning; I anchored this analysis in the EU legal framework, and followed a law and society approach to speculate on the factors that enhanced the emergence of the limbs contained in the legal formulation of the rights to respect for private and family life and personal data protection. I demonstrated that both rights

are instrumental in fostering personhood, one's unique identity, protected as an expression of dignity. As such rights emerged out of modernity, they enabled the autonomy crucial for maintaining that democratic society expression of the Union *ordre public*. Contextually, I defended the significance and independence of the right to the protection of personal data.

The second challenge asked whether security and privacy are the only relevant dimensions to be taken into account. By looking at specific offences, rather than simply 'security', it emerged that offences-related actions may be implemented through technology. Likewise, I noted that technology might be viewed as an intervening variable affecting the two privacy rights, which can not only encroach on them (irrespective of the fight against crime), but in certain circumstances also safeguard them. The specific impact of technology, however, required the analysis of concrete measures.

The third challenge concerned both whether giving up privacy is the most efficient solution to achieve security, and why, which requires a parameter for efficiency. In the light of the instrumental value of security in protecting those rights underlining the Union *ordre public*, I noted that the efficiency of trading-off privacy rights for security becomes questionable.

Since the relationship between security and privacy rights would have to be appraised, on a case-by-case basis, in relation to specific offences, I moved onto analysing cybersecurity, my case study, as understood in Union law, i.e. as network and information security (NIS) and the fight against cybercrime (chapter 3). The case of cybercrime/NIS is particularly interesting for its ambiguity as to the relationship between security and privacy rights, not least because of the technology involved. On the one hand, the protection of networks and information systems seems to converge with safeguarding personal data and private communications travelling on the Internet, which has national security import due to the reliance of critical infrastructure on networks. On the other hand, privacy rights are in tension with the pursuit of national security objectives in cyberspace, and the need to collect data as evidence, as shown by Snowden's revelations. The latter remained an issue even after rebutting the trade-off model on the basis of the normative challenge. Following the steps of the methodological challenge, I proposed to reformulate the relationship between 'cybersecurity' and 'privacy rights' *vis-à-vis* the NIS Directive, the eIDAS Regulation, the Directive on Attacks against Information Systems, the Council Framework Decisions against fraud, the anti-child abuse Directive, the proposed counterterrorism Directive, and the Directive against Human Trafficking. The analysis also revealed the fickle legal meaning of the concept of cybercrime.

The reformulations of the trade-off supported my second assumption: i.e., that narrow cybercrime would seem to equate with the absence of information security, and would thus require preventive approaches based on technology. In addition, broad cybercrime is the substantiation of crimes whose prevention requires societal action and education (chapter 4). As a result, I therefore grouped the relationships between 'cybersecurity' and 'privacy rights' derived from the applicable law into two groups, narrow cybercrime/NIS and broad cybercrime. There, it became clear that technology, featuring on both sides of the equation 'security v. privacy', leads to the possibility of complementarity between narrow cybercrime/NIS and privacy rights as advanced in hypothesis II. As for the 'how' question, the legal analysis seemed to support the argument for general convergence and, in the case of data breaches, overlap, corroborating hypotheses IIa and IIb. Causality could not be proved without reference to specific technologies, leaving hypothesis IIc unanswered. The analysis seemed to confirm my second assumption, whereby narrow cybercrime and broad cybercrime raise similar evidentiary issues: when it comes to 'data' as evidence, the law seems to favour limiting privacy rights for the sake of the fight against crime; this may challenge the correctness of hypothesis IIIa, to prove which it is necessary to look into technological solutions.

This led to the analysis of broad cybercrimes, which seemed to confirm their tension with privacy rights, and hence resort to specific measures would have to be assessed by means of permissible limitations. A positive factor in the direction of reconciliation (hypothesis IIIb) is the recently adopted Directive on the protection of personal data in the AFSJ. However, the analysis showed the difficulty of finding a concrete answer regarding the nature of the relationship without considering specific measures, given the breadth of options that are available for investigative purposes. Moreover, not only do some of these investigative options encroach on privacy, but they also seem to lead to the commission of narrow cybercrimes, thus threatening NIS and raising serious questions of efficiency.

On the one hand, the analysis of the reformulation of 'security v. privacy' in the context of narrow cybercrimes/NIS, and broad cybercrimes, proved hypothesis I right. Being over-simplistic, the trade-off obscures a crucial factor – technology – and fails to capture important dimensions of the relationship between security and privacy, such as complementarity, and cases in which a trade-off could lead to highly inefficient, if not catastrophic, results (let alone the fact that it excludes the possibility that sufficient guarantees in law would mediate the outcome). On the other hand, the analysis showed the need to factor in technology in order to

provide firmer answers to the hypotheses. As such, I chose to analyse deep packet inspection, as a measure useful for addressing both narrow cybercrime/NIS and broad cybercrime. DPI, looked at from the perspective of applicable law, appeared to be variously capable of both protecting and infringing privacy rights, leading to the paradox of the same technology being both permissible and impermissible, and to a seeming impasse. This introduced hypothesis IV, whereby I identified the problem as lying in technology neutrality, the courts' avoidance of pronouncing on matters of technology, and the open-ended understanding of privacy rights.

To appraise whether cybersecurity and privacy rights can be reconciled, I proposed bridging the technological and legal understandings of information security and privacy (chapter 5). After a review of existing research, I proposed a five-step methodology. The first step consists in building a matrix based on mapping the correspondence of cybercrimes, as defined in EU applicable law, to existing, real world threats and the technologies used to perpetrate, prevent-detect and detect-investigate them. In other words, I suggested linking existing literature on threats and technologies to legal definitions of cybercrimes. The second step was to appraise the impact of such technologies on information security and privacy, technically understood. I established a link between the technologies, information security canons and privacy canons, by relying on STRIDE and LINDDUN respectively, and on-going work on privacy by design. The third step was to assess whether these technologies are susceptible to interfere with privacy rights and their essence or core, for which I followed three steps. To understand the meaning of fundamental rights, I suggested performing the exercise, in the abstract, of dissecting the right into its substantive characteristics or attributes – an idea taken from, and building upon, work on indicators. On that basis, it was possible to identify the essence or core of the right, based on the revisited core-periphery theory of fundamental rights of Alexy, the intrusion into which would be prohibited. Finally, I proposed linking the technologies analysed to their impact both on privacy canons and the attributes (core) of rights. The fourth step consisted in appraising the permissibility of such technologies, based on the type of impact and level of intrusion they have on privacy rights, and hence the balancing/proportionality test enhanced by the core-periphery model. The final step was to compare the technologies on the basis of their impact on privacy and cybercrime, to appraise whether strategies to protect the first and prevent the second are complementary, or rather whether there is a tension. I suggested the SURVEILLE method could be used as a method for coding technologies, which could then be grouped according to Clarke's revisited

taxonomy: interference, compliance and synergy. The SurPRISE method could then be used to select the most adequate technologies.

Following the proposed method, I identified the attributes of the right to respect for private and family life, as a corrected version of those found by the UK Human Rights Management Framework, and I proposed potential core areas (chapter 6). I found the following attributes: private life (physical and psychological integrity – excluding in the context of medicine and biology; personal social and sexual identity; and personal development, autonomy and participation); (Confidential) communications; family life; and Home. Therein, I also proposed a test for permissible limitations specific to the EU.

I then embarked on an experimental identification of attributes of the right to the protection of personal data, based on the methodology of indicators and the established debate on FIPs (chapter 7). Even more experimentally, I proposed the identification of cores. I found the following attributes: Legitimate processing (attribute of the rule of law); Oversight (supervisory authority and human intervention); Data subjects' rights; Minimization and accuracy; and Security. Sensitive data were not considered as a separate attribute, but as capable of lowering the threshold of permissible interferences. At the same time, I set to demonstrate the independence, in EU law, of the right to the protection of personal data.

The identification of attributes was then crossed with the technological understanding of privacy and information security protection goals (chapter 8). The analysis reinforced the idea of convergence/overlap between narrow cybercrime/NIS and privacy rights found in chapter 4, but it also showed cases leading to a potential clash, which need to be taken into account. Importantly, some clashes could concern the right to respect for private life with the protection of personal data, to the effect of reinforcing their independence.

This analysis was a preliminary step to a trial run of the method, which I chose to apply on an example of narrow cybercrime, i.e. illegal data interference. Unlike illegal interception, which is widely discussed in the literature as harbouring a convergence between privacy and information security, or illegal access (data breaches), which in the legal analysis resulted in an overlap between privacy rights and NIS, illegal data interference was less 'obvious' and enabled the study of an off-the-shelf DPI engine, which connects with the analysis conducted in chapter 4.

The trial run confirmed the possibility, suggested in chapter 4, that measures used to tackle narrow cybercrime/NIS could infringe privacy, thus defying hypothesis II and IIIa. However, DPI only acted as a 'straw in the wind' test: a final answer on the hypothesis would only result from a sufficiently large N, after performing step 5 of the methodology, i.e. assigning values according to the SURVEILLE method, and ranking methods according to their permissibility. This begs the question of which model of reconciliation (if any) is more likely, which I address below.

2 THREE SCENARIOS FOR THE RESEARCH QUESTION

The results of the trial run are illustrative and experimental: the N is clearly too small, and at the same time the method must be peer-reviewed and validated (by the legal and computer science community). Although this analysis cannot provide a final answer to the research question, as a more developed matrix is needed to provide a doubly-decisive test (i.e. information that is both necessary and sufficient to prove the research question), it can be said that performing the fully-fledged methodology will lead to one of the three scenarios discussed below. Each bears different implications for research and policy.

In the first scenario (the best-case scenario), a doubly decisive test confirms the hypotheses. In other words, the method works at the technological level and, in the aggregate, it shows integration between narrow cybercrime prevention/NIS and privacy rights. The following could be assumed: namely, that the method is promising, and testing it on more cases would be needed to demonstrate robustness. Policy-wise, it would show the need to tackle cybersecurity and 'privacy' together, giving pre-eminence to NIS over broad cybercrime-related considerations, thus finding a way to overcome the diffidence of the diverse communities.

According to a second scenario (the worst-case scenario), the method would not work, and nothing could be said about the hypotheses. This conclusion would lend strong support to the need to resort to classic balancing and rely heavily on judgments to contest policy decisions. The research question would bear a negative answer.

Pursuant to a third scenario (middle-case scenario), **the method works, but the hypotheses are challenged.** The method could work at the technological level but, in the aggregate, it would show ambiguity in the relationship between narrow cybercrime prevention/NIS and privacy rights. The following could be assumed: that the method is promising, and testing it on more cases would be needed to demonstrate robustness. It would not, however, be possible to make unambiguous claims about integrating the two rights within a cybersecurity policy. The research question would be, at most, impossible to answer once and for all.

This could actually be the most likely scenario, *vis-à-vis* a reality in which the market is left free to develop tools as it sees fit. The relationship between cybersecurity and privacy rights could follow several blueprints depending on the crime at hand. Any of Clarke's categories of technological impact on privacy rights - interference, compliance and synergy- could be of use here. As for causality, the most difficult hypothesis to prove (hypothesis IIc), there could be a Russian-doll style relationship, whereby the adoption of progressively protective measures would benefit NIS, protection of personal data, private life, etc.

The fact that 'interference' may be part *de facto* of the relationship between cybersecurity and privacy rights paves the way to important policy reflections. Before illustrating them, I first demonstrate the research significance of testing the method (and this thesis at large).

3 SIGNIFICANCE OF TESTING THE METHOD

3.1 RESEARCH-RELATED REFLECTIONS

An important research outcome of testing the method concerns the notion of essence or core areas of the right. Is interference inherent in the absence, thus far, of privacy by design approaches to technology, or does it have to do with the undefined contours of rights? The idea that the content of communications is the essence of the right to respect for private and family life is a case in point. It may also lead to a completely new understanding of the notion of essence, which could be procedural, rather than substantive.

A second research reflection concerns the feasibility of the method. As I stated above, the methodology can be widely tested only after it has been peer-reviewed and validated. Such an exercise is feasible, but requires means that are beyond a PhD thesis. It calls for trans-disciplinary cooperation between computer scientists and lawyers, decent funding and a time span of at least one year.

3.1.1 Research Reflections beyond the method

The development of my argument throughout the thesis brought to surface very interesting questions. Addressing those questions would have taken me off road: thus, and sadly, I had to renounce the company of those issues in the journey that was my thesis. However, I wish to give credit to such potential companions, as they kept my intellectual curiosity awake, and will hopefully inform new, exciting intellectual expeditions.

One set of questions concerns whether the CJEU shows a bias in favour of technology, thus *de facto* sanctioning societal acceptance. My analysis was limited to privacy rights. Addressing such a question would require empirical legal studies, and expanding the analysis to other rights and additional case studies. A related question is the extent to which the collection of scientific evidence in the context of judgments issued by the CJEU is appropriate and sufficient.

A second set of questions concerns the broader subject of the 'regulation of technology'. To what extent is the 'risk management/assessment' paradigm, shared by privacy rights and information security, an inherent feature testifying to their convergence? Or is the notion of 'risk' a hidden regulatory factor, which has led down a one-way alley?

Thirdly, the object of this research could be observed from alternative angles. One such angle is the relationship between SIGINT and cybersecurity, which would obviously take the reasoning to a higher level of abstraction, and force us to reflect on the defensive/offensive nexus of state power and the related constitutional architecture.

A fourth and important question concerns whether the level of protection offered by the ECHR and CJEU in privacy cases differs in practice. It would mean choosing comparable

cases, on the basis of which the two courts' decisions should be appraised. This would have a bearing on the question as to whether article 7 of the Charter overlaps with article 8 ECHR.

A final question is a study of the regulatory instruments analysed in this thesis from the perspective of technology neutrality, for instance based on the parameters identified by Reed and Koops. What kind of approach to technology is the EU following? Are we unknowingly embracing techno-regulation, and sleepwalking into modulated democracy? And what does this mean for the EU's *ordre public*?

3.2 POLICY-RELATED REFLECTIONS AND SIGNIFICANCE

A potential outcome of running the method, which bridges research and policy, is that it could pave the way to a human rights indicator, as anticipated in chapter 5. Human rights indicators are a method geared at evaluating and overseeing states' duty to promote and protect human rights.[1293] They are "specific information on the state of an event, activity or an outcome that can be related to human rights norms and standards; that address and reflect the human rights concerns and principles."[1294] As such, they can concern technologies, but their purview is all-encompassing. The use of human rights indicators at the institutional level has been hampered by the lack of a coherent framework for their development and use. Quantitative approaches have also been viewed with suspicion, in the fear that this could lead to ranking or prioritizing what is considered as an indivisible catalogue of human rights, and to dismiss unquantifiable qualitative features. The work of, among others, the United Nations' OHCHR, supported by the FRA,[1295] filled the gap in the literature, by giving equal value to the qualitative and quantitative criteria.[1296] Good indicators are jurisdiction-specific: for the case in hand, the indicator could prove compliance with privacy rights in the fight against cybercrime within the AFSJ. Such analysis could be extended to other fundamental rights, which could also be dissected into attributes and cores, as discussed in chapter 6. An indicator could be a policy-relevant tool, enabling the decision of permissible or impermissible technologies. This links to other policy outcomes.

[1293] United Nations (2006), p. 3.
[1294] Ibid.
[1295] Fundamental Rights Agency (2001), *Using indicators to measure fundamental rights in the EU: challenges and solutions*.
[1296] United Nations (2012), p. 27.

An additional policy outcome, anticipated in the conclusions to chapter 8, is that a trial run of the method unveiled an unforeseen aspect of the 'how' question: it showed that complementarity between narrow cybercrime/NIS may in some circumstances only be achieved with some 'interference'. Given such interference, reconciliation could only ensue as a result of choosing the most adequate measure, i.e. the least intrusive one, used under appropriate safeguards. Building on the insight of the SURVEILLE project, a *prima facie* impermissible measure could become permissible if authorized by an instrument providing sufficient safeguards, as well as the implementation of privacy by design approaches, which will become mandatory both in the internal market and in the AFSJ (article 20 of the Directive on data protection in the AFSJ). These combined reflections meet at the intersection of the need for applicable law that addresses explicitly issues of adequacy, safeguards and design.

Instruments currently in force, and even recently adopted, seem unsatisfactory in this respect. One such instrument is the NIS Directive, which failed the test set by *Digital Rights Ireland*, insofar as monitoring is concerned.

The absence of suitable law, whether because it is technology neutral to the point of irrelevance, or because it lacks the necessary safeguards, has two intertwined effects that have a bearing on the reconcilability of technology (used to pursue security goals) with rights.

First, it leaves the market free to find sub-standard solutions that silently violate fundamental rights (techno-regulation, chapter 8, section 3). This can have a bearing on the reconcilability of cybersecurity with privacy rights, or otherwise on a reality where the two are artificially opposed, and pulled to the whims of different communities (whose interests may converge at the detriment of the individual and her privacy rights).

Second, and relatedly, market solutions found in the silence of the law to shield users from intrusive technologies may lead to sub-optimal societal outcomes that, for instance, exacerbate the tension between privacy rights and broad cybercrimes. And this is a second way in which reconciliation is affected: technology kills the trade-off model, but it raises new issues. There is no 'invisible hand' (in the market) of technology, but rather the very cumbersome presence of a military-industrial complex that is pushing developments in a risky direction. It is the job of law and politics to re-appropriate decision-making as to which values technology should pursue. This may mean ceasing to hide behind 'technology neutrality' in law-making, and indifference towards technology in case law.

To finish on a positive note, a glimpse of hope has come from the EDPS, which has set up an external ethics advisory group to 'explore the relationships between human rights, technology, markets and business models in the 21st century', and help indicate the issues that should be subject to a political process.[1297] We need to rethink our approach to regulating technology, so that technology will not make regulation – and privacy rights, and NIS – obsolete.

[1297] Executive Summary of the Opinion of the European Data Protection Supervisor on 'Meeting the challenges of big data: a call for transparency, user control, data protection by design and accountability'.

BIBLIOGRAPHY

1 PRIMARY SOURCES

1.1 CASE LAW

1.1.1 JUDGMENTS OF THE CJEU

Judgment of 17 December 1970 in Internationale Handelsgeselleschaft mbH v. Einfuhr- und Vorratsstelle für Getreide und Futtermittel, C-11/70, EU:C:1970:114

Judgment of 14 May 1974 in Nold KG v. European Commission, C-4/73, EU:C:1974:51

Judgment of 4 December 1974 in Van Duyn v. Home Office, C-41/74, EU:C:1974:133

Judgment of 28 October 1975 in Rutili v. Ministre de l'intérieur, C-36/75, EU:C:1975:137

Judgment of 26 June 1980 in National Panasonic v. Commission, C-136/79, EU:C:1980:169

Judgment of 12 November 1981 in Meridionale Industria Salumi and Others, Joined cases 212 to 217/80, EU:C:1981:270

Judgment of 23 April 1986 in Les Verts v. Parliament, C-294/83, EU:C:1986:166

Judgment of 13 July 1989 in Wachauf v. Bundesamt Für Ernährung Und Forstwirtschaft, C-5/88, EU:C:1989:321

Judgment of 21 September 1989 in Hoechst v. Commission, Joined cases 46/87 and 227/88, EU:C:1989:337

Judgment of 5 May 1998 in United Kingdom v. Commission, C-180/96, EU:C:1998:192

Judgment of 13 April 2000 in Karlsson and Others, C- 292/97, EU:C:2000:202

Judgment of 14 September 2000 in Fisher, Case C-369/98, EU:C:2000:443

Judgment of 20 May 2003 in Österreichischer Rundfunk and Others, Joined cases C-465/00, C-138/01 and C-139/01, EU:C:2003:294

Judgment of 12 June 2003 in Schmidberger, C-112/00, EU:C:2003:333

Judgment of 6 November 2003 in Bodil Lindqvist, C-101/01, EU:C:2003:596

Judgment of 29 April 2004 in Commission v. CAS Succhi di Frutta, C-496/99 P, EU:C:2004:236

Judgment of 30 May 2006 in Parliament v. Council, Joined Cases C-317/04 and C-318/04, EU:C:2006:346 (PNR cases)

Judgment of 18 January 2007 in PKK and KNK v. Council, C-229/05 P, EU:C:2007:32

Judgment of 29 January 2008 in Promusicae, C-275/06, EU:C:2008:54

Judgment of 25 July 2008 in Metock and Others, C-127/08, EU:C:2008:449

Judgment of 3 September 2008 in Kadi and Al Barakaat International Foundation v Council and Commission, Joined Cases C-402/05 P and C-415/05, EU:C:2008:461 (Kadi I)

Judgment of 10 February 2009 in Ireland v. Parliament and Council, C-301/06 EU:C:2009:68 (Data Retention I)

Judgment of 4 March 2010 in Chakroun, C-578/08, EU:C:2010:117

Judgment of 9 March 2010 in European Commission v. Federal Republic of Germany, C-518/07, EU:C:2010:125
Judgment of 29 June 2010 in Bavarian Lager Ltd, C-28/08 P, EU:C:2010:378
Judgment of 5 October 2010 in McB, C-400/10 PPU, EU:C:2010:582
Judgment of 9 November 2010 in Schecke and Eifert, C-92/09 and C-93/09, EU:C:2010:662
Judgment of 22 December 2010 in Ilonka Sayn-Wittgenstein v. Landeshauptmann von Wien, C-208/09, EU:C:2010:806
Judgment of 22 December 2010 in Mercredi, C-497/10 PPU, EU:C:2010:829
Judgment of 5 May 2011 in Deutsche Telekom, C-543/09, EU:C:2011:279
Judgment of 12 May 2011 in Runevič-Vardyn and Wardyn, C-391/09, EU:C:2011:291
Judgment of 15 November 2011 in Dereci and others v. Bundesministerium für Inneres, C-256/11, EU:C:2011:734
Judgment of 24 November 2011 in Scarlet Extended, C-70/10, EU:C:2011:771
Judgment of 24 November 2011 in ASNEF and FECEDM, joined cases C-468/10 and C-469/10, EU:C:2011:777
Judgment of 16 December 2011 in Satakunnan and Satamedia, C-73/07, EU:C:2008:727
Judgment of 21 December 2011 in Commission v. Austria, C-28/09, EU:C:2011:854
Judgment of 16 February 2012 in Sabam, C-360/10, EU:C:2012:85
Judgment of 19 July 2012 in Parliament v. Council, C-130/10, EU:C:2012:472
Judgment of 16 October 2012 in Commission v. Austria, C-614/10, EU:C:2012:631
Judgment of 16 October 2012 in Hungary v. Slovakia, C-364/10, EU:C:2012:630
Judgment of 30 May 2013 in Worten, C-342/12, EU:C:2013:355
Judgment of 4 June 2013 in ZZ, C-300/11, EU:C:2013:363
Judgment of 6 June 2013 in Ayadi v. Commission*, C-183/12 P, EU:C:2013:369*
Judgment of 17 October 2013 in Schwarz, C-291/12, EU:C:2013:670
Judgment of 7 November 2013 in X and Others, Joined Cases C-199/12 to C-201/12, EU:C:2013:720
Judgment of 7 November 2013 in IPI, C-473/12, EU:C:2013:715
Judgment of 12 December 2013 in X, C-486/12, EU:C:2013:836
Judgment of 12 March 2014 in Al Assad v. Council, T-202/12, EU:T:2014:113
Judgment of 13 May 2014 in Google Spain and Google, C-131/12, EU:C:2014:317
Judgment of 8 April 2014 in Commission v. Hungary, C-288/12, EU:C:2014:237
Judgment of 8 April 2014 in Digital Rights Ireland and Seitlinger and Others, Joined cases C-293/12 and C-594/12, EU:C:2014:238
Judgment of 17 July 2014 in YS and others, Joined cases C-141/12 and C-372/12, EU:C:2014:2081
Judgment of 2 October 2014 in U, C-101/13, EU:C:2014:2249
Judgment of 2 December 2014 in A, B, and C, Joined cases C-148/13 to C-150/13, EU:C:2014:2406
Judgment of 11 December 2014 in Ryneš, C-212/13, EU:C:2014:2428
Judgment of 16 April 2015 in Willems, Joined Cases C-446/12 to C-449/12, EU:C:2015:238
Judgement of 15 July 2015 in Dennekamp v. Parliament, T-115/13, EU:T:2015:497
Judgment of 16 July 2015 in Lanigan, C-237/15 PPU, EU:C:2015:474

Judgment of 1 October 2015 in Weltimmo, C-230/14, EU:C:2015:639
Judgment of 6 October 2015 in Schrems, C-362/14, EU:C:2015:650
Judgment of 17 December 2015 in WebMindLicenses, C-419/14, EC:C:2015:832
Judgment of 17 December 2015 in Åkerberg Fransson, C-617/10, EU:C:2013:105
Judgment of 14 June 2016 in Parliament v. Council, C-263/14, EU:C:2016:435, para 47
Opinion of Advocate General Bot of 30 January 2014 in European Parliament v. Council, C-658/11, EU:C:2014:41
Opinion of Advocate General Sharpston of 17 July 2014 in A, B and C, Joined Cases C‑148/13, C‑149/13 and C‑150/13, EU:C:2014:2111
Opinion of the Court of 18 December 2014, Avis 2/13, EU:C:2014:2454
Opinion of AG Saugmandsgaard Øe of 19 July 2016 in Tele2 Sverige and Watson and others, Joined cases C-203/15 and C-698/15, EU:C:2016:572
Order of 16 July 2015 in Sánchez Morcillo and Abril García, C-539/14, EU:C:2015:508

1.1.2 JUDGMENTS OF THE ECTHR (BY DECISION DATE AS IN THE ECLI)

Golder v. the United Kingdom, n. 4451/70, CE:ECHR:1975:0221JUD000445170
Klass and others v. Germany, n. 5029/71, CE:ECHR:1978:0906JUD000502971
Marckx v. Belgium, n. 6833/74, CE:ECHR:1979:0613JUD000683374
X and Y v. the Netherlands, n. 8978/80, CE:ECHR:1985:0326JUD000897880
Judge Pettiti, concurring opinion in Malone v. the United Kingdom, n. 8691/79, CE:ECHR:1985:0426JUD000869179
Leander v. Sweden, n. 9248/81, CE:ECHR:1987:0326JUD000924881
Berrehab v. The Netherlands, n. 10730/84, CE:ECHR:1988:0621JUD001073084
Eriksson v. Sweden, n. 11373/85, CE:ECHR:1989:0622JUD001137385
Moustaquim v. Belgium, n. 12313/86, CE:ECHR:1991:0218JUD001231386
Herczegfalvy v. Austria, n. 10533/83, CE:ECHR:1992:0924JUD001053383
Olsson v. Sweden, n. 13441/87, CE:ECHR:1992:1127JUD001344187
Niemietz v. Germany, n. 13710/88, CE:ECHR:1992:1216JUD001371088
Esbester v. the United Kingdom, n. 18601/91, CE:ECHR:1993:0402DEC001860191
C v. Belgium, n 21794/93, CE:ECHR:1996:0807JUD002179493
Halford v. the United Kingdom, n. 20605/92, CE:ECHR:1997:0625JUD002060592
Herbecq and the Association "Ligue Des Droits De L'homme" v. Belgium, n. 32200/96 and 32201/96, CE:ECHR:1998:0114DEC003220096 (European Court of Human Rights)
Rotaru v. Romania, n. 28341/95, CE:ECHR:2000:0504JUD002834195
PG and JH v. the United Kingdom, n. 44787/98, CE:ECHR:2001:0925JUD004478798
Pretty v. the United Kingdom, n. 2346/02, CE:ECHR:2002:0429JUD00234602 (tentative)
Mikulić v. Croatia, n. 53176/99, CE:ECHR:2002:0207JUD005317699
Peck v. the United Kingdom, n. 44647/98, CE:ECHR:2003:0128JUD004464798
Perry v. the United Kingdom, n. 3737/00, CE:ECHR:2003:0717JUD006373700
M C v. Bulgaria, n 39272/98, CE:ECHR:2003:1204JUD003927298

Perrin v. the United Kindgom, n. 5446/03, CE:ECHR:2005:1018DEC000544603
Copland v. the United Kingdom, n. 62617/00, CE:ECHR:2007:0403JUD006261700
KU v. Finland, n 2872/02, CE:ECHR:2008:1202JUD000287202
Iordachi and Others v. Moldova, n. 25198/02, CE:ECHR:2009:0210JUD002519802
Shimovolos v. Russia, n. 30194/09, CE:ECHR:2011:0621JUD003019409
X and Others v. Austria, n. 19010/07 CE:ECHR:2013:0219JUD001901007
Bernh Larsen Holding As and Others v. Norway, n 24117/08, CE:ECHR:2013:0314JUD002411708
Stolyarova v. Russia, n. 15711/13, CE:ECHR:2015:0129JUD001571113
Szabó and Vissy v. Hungary, n. 37138/14, CE:ECHR:2016:0112JUD003713814
Big Brother Watch and others, *Joint Application under Article 34* (n. 58170/13, 2013)

1.1.3 JUDGMENTS OF THE HRC

Singh Bhinder v. Canada, Communication n. 208/1986, CCPR/C/37/D/208/1986
Sayadi and Vinck v. Belgium, Communication n. 1472/2006, CCPR/C/94/D/1472/2006

1.1.3.1 Comments

Human Rights Committee, *Comments of the Human Rights Committee: United Kingdom of Great Britain and Northern Ireland* (CCPR/C/79/Add 55, 1979)
——, *General Comment n. 16. Article 17 (The right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation)* (1988)
——, *General Comment n. 27. Freedom of Movement (Article 12)* (CCPR/C/21/Rev1/Add9, 1999)
——, *General Comment n. 31, The Nature of the General Legal Obligation* (2004)
——, *General Comment No. 32. Article 14: Right to Equality Before Courts and Tribunals and to a Fair Trial* (CCPR/C/GC/32, 2007)
——, *General Comment n. 34. Article 19: Freedoms of Opinion and Expression* (CCPR/C/GC/34, 2011)
——, *General Comment n. 35. Article 9 (Liberty and security of person)* (CCPR/C/GC/35, 2014)

1.1.4 JUDGMENTS - OTHER COURTS

Volkszählungsurteil, 65 BVerfGE, 1, Bundesverfassungsgericht - German Federal Constitutional Courts, 15 December 1983
BVerfG, 2 BvE 2/08 Rn (1-421), Judgment of 30 June 2009
Concurring opinionof Judge Scalia in the case of City Of Ontario, California, et al. v. Quon et al. Supreme Court Of The United States, Syllabus Certiorari To The United States Court Of Appeals For The Ninth Circuit, No. 08–1332, 17 June 2010

1.2 LEGAL INSTRUMENTS

1.2.1 EU LAW

1.2.1.1. Primary law

Charter of Fundamental Rights of the European Union, OJ C 303/01

Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU) (Lisbon Treaty) OJ C 83/01

1.2.1.2 Secondary law

Commission Regulation 611/2013/EU of 24 June 2013 on the Measures Applicable to the Notification of Personal Data Breaches under Directive 2002/58/EC of the European Parliament and of the Council on Privacy and Electronic Communications (Commission Regulation on Data Breaches)

Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the Signing, on Behalf of the European Union, of an Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement)

Council Decision 2009/902/JHA of 30 November 2009 Setting up a European Crime Prevention Network (EUCPN) and repealing Decision 2001/427/JHA, OJ L 321

Council Decision 2010/16/CFSP/JHA of 30 November 2009 on the Signing, on behalf of the European Union, of the 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 Purposes of the Terrorist Finance Tracking Program, OJ L 8 (TFTP Agreement)

Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection, OJ L 345

Council Framework Decision 2002/475/JHA of 13 June 2002 on Combating Terrorism, OJ L 164

Council Framework Decision 2006/960/JHA of 18 December 2006 on Simplifying the Exchange of Information and Intelligence between Law Enforcement Authorities of the Member States of the European Union, OJ L 386

Council Framework Decision 2008/913/JHA of 28 November 2008 on Combating Certain Forms and Expressions of Racism and Xenophobia by Means of Criminal Law, OJ L 328

Council Framework Decision 2008/919/JHA of 28 November 2008 Amending Framework Decision 2002/475/JHA on Combatting Terrorism (Framework Decision on Terrorism) OJ L 330

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

Council Regulation 881/2002/EC of 27 May 2002 Imposing Certain Specific Restrictive Measures Directed Against Certain Persons and Entities Associated with Usama bin Laden, the Al-Qaida Network and the Taliban, and Repealing Council Regulation (EC) No 467/2001 Prohibiting the Export of Certain Goods and Services to Afghanistan, Strengthening the Flight Ban and Extending the Freeze of Funds and Other Financial Resources in Respect of the Taliban of Afghanistan, OJ L 139

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 (Data Protection Directive) OJ L 281

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), OJ L 178

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive), OJ L 108

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 (e-Privacy Directive) OJ L 201

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 (Data Retention Directive) OJ L 105/54

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 n. 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws, OJ L 337

Directive 2009/140/EC of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services OJ L 337.

Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on Preventing and Combating Trafficking in Human Beings and Protecting its Victims, and Replacing Council Framework Decision 2002/629/JHA, OJ L 101

Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing Council Framework Decision 2004/68/JHA, OJ L 335

Directive 2013/40/EU of the European Parliament and the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA, OJ L 218

Directive 2015/1535/EU of the European Parliament and of the Council of 9 September 2015 Laying down a Procedure for the Provision of Information in the Field of Technical Regulations and of Rules on Information Society services (codification), OJ L 241

Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) n. 1093/2010, and repealing Directive 2007/64/EC, OJ L 337

Directive 2016/680/EU of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data, and Repealing Council Framework Decision 2008/977/JHA, OJ L 119/89

Directive 2016/681/EU of the European Parliament and of the Council of 27 April 2016 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime (PNR Directive) OJ L 119

Directive 2016/1148/EU of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, OJ L 194

Explanations Relating to the Charter of Fundamental Rights, OJ C 303/02 (Explanations to the Charter)

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 L 8

Regulation 526/2013/EU of the European Parliament and the Council of 21 May 2013 Concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) n. 460/2004

Regulation 513/2014/EU of the European Parliament and of the Council of 16 April 2014 Establishing, as Part of the Internal Security Fund, the Instrument for Financial Support for Police Cooperation, Preventing and Combating Crime, and Crisis Management and Repealing Council Decision 2007/125/JHA, OJ L 150/93

Regulation 910/2014/EU of the European Parliament and Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, OJ L257

Regulation 2015/2120/EU of the European Parliament and of the Council of 25 November 2015 Laying down Measures Concerning Open Internet Access and Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services and Regulation (EU) 531/2012 on Roaming on Public Mobile Communications Networks within the Union

Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free

Movement of such data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1

Regulation 2016/794/EU of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135

1.2.1 INTERNATIONAL LAW INSTRUMENTS

1.2.2.1. Council of Europe

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, Council of Europe, CETS n.181, 8 November 2001

Additional Protocol to the Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, Council of Europe, ETS n. 189

Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocols No 11 and 14), Council of Europe, ETS n° 005, 4 November 1950

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS n. 108, 28 January 1981

Convention on Cybercrime, Council of Europe, CETS n. 105 23 November 2001

Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Council of Europe (2016)

Explanatory Memorandum of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe

1.2.1.2 United Nations

Universal Declaration of Human Rights (UDHR). General Assembly of the United Nations, Resolution 217, 10 December 1948

International Covenant on Civil and Political Rights, I-14668, UNTS n° 999

1.2.1.3 Instruments of soft law

Council of Europe, *Memorandum of Understanding between the Council of Europe and the European Union CM(2007)74 1* (117th Session of the Committee of Ministers, 2007)

—, *Guidelines for the Cooperation between Law Enforcement and Internet Service Providers against Cybercrime, Adopted by the Global Conference Cooperation against Cybercrime* (2008)

International Organization for Standarization (ISO), *International Standard ISO/IEC 29100:2011(E) Information technology — Security techniques — Privacy framework* (2011)

Organization for Economic Cooperation and Development (OECD), *Recommendation on Guidelines for the Security of Information and Networks. Towards a Culture of Secuirty* (2002)

Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Organization for the Economic Cooperation and Development, C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79

United Nations, General Assembly, *Declaration on Principles of International Law Friendly Relations and Co-Operation Among States in Accordance with the Charter of the United Nations* (1970)

——, *Declaration on the Use of Scientific and Technological Progress in the interest of Peace and for the benefit of Mankind (Teheran Declaration)* (Thirtieth Session, 2400th plenary meeting, 1975)

United Nations, General Assembly *Resolution the right to Privacy in the Digital Age, A/RES/68/167* (2013)

1.2.1.4 Preparatory works

Council of Europe, European Commission of Human Rights, 'Preparatory work on Article 8 of the European Convention on Human Rights' < http://www.echr.coe.int/library/COLFRTravauxprep.html>

United Nations, Economic and Social Council, *Commission on Human Rights Drafting Committe. International Bill of Rights* (E/CN4/AC1/3/ADD1 Part 1, 1947)

2 SECONDARY SOURCES

2.1 ACADEMIC LITERATURE

Abele Robert P., *A Users' Guide to the USA Patriot Act and Beyond* (University Press of America 2005)

Abelson Harold and others, 'Keys under doormats: mandating insecurity by requiring government access to all data and communications' (2015) 0 Journal of Cybersecurity 1-11

Ackerman Bruce, *Before the Next Attack. Preserving Civil Liberties in an Age of Terrorism.* (Yale University Press 2006)

Adams Maurice and others (eds), *Judging Europe's Judges. The legitimacy of the case law of the European Court of Justice* (Hart Publishing 2013)

Adams Samantha and others, *The Governance of Cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK* (Tilburg University, 2015)

Alexy Robert, 'Constitutional Rights and Legal Systems' in Nergelius Joakim (ed), *Constitutionalism - New Challenges: European Law from a Nordic Perspective* (Brill 2008)

Alston Philip, Bustelo Mara and Heenan James (eds), *The EU and Human Rights* (Oxford University Press 1999)

Anderson David and Murphy Cian C, 'The Charter of Fundamental Rights' in Biondi Andrea, Eeckhout Piet and Ripley Stefanie (eds), *EU Law After Lisbon* (Oxford Scholarship Online 2012)

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

Anderson Ross and others, 'Measuring the Cost of Cybercrime' in Böhme Rainer (ed), *The Economics of Information Security and Privacy* (Springer 2012) <http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf>

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

Andrade Norberto, 'The Right to Personal Identity in the Information Age. A reappraisal of a lost right' (PhD thesis, European University Institute 2011)

Angelini Francesca, *Ordine pubblico e integrazione costituzionale europea. I princìpi fondamentali nelle relazioni interordinamentali* (Cedam 2007)

Arendt Hannah, 'Freedom and Politics: a lecture' (1960) 14 Chicago Review 28-46

——, *The Origins of Totalitarianism* (Harcourt 1968)

——, *The Human Condition (2nd edition)* (The University of Chicago Press 1998)

Armbrust Michael and others, *Above the Clouds: A Berkeley View of Cloud Computing.* (Technical Report No UCB/EECS-2009-28, 2009)

Bagnasco Arnaldo, Barbagli Marzio and Cavalli Alessandro, *Sociologia, Cultura e Società. I concetti di base* (Il Mulino 2001)

Barland Marianne and others, *Report on decision support testing* (SurPRISE Project Deliverable D 7.1 2014)

Beck Ulrich, 'La société du risque globalisé revue sous l'angle de la menace terroriste' (2003) 114 Cahiers Internationaux de Sociologie p. 22

Becker Georg T. and others, 'Stealthy Dopant-Level Hardware Trojans' in Bertoni Guido and Coron Jean-Sébastien (eds), *Cryptographic Hardware and Embedded Systems - CHES 2013* (Springer 2013)

Bendrath Ralf, 'Global Technology Trends and National Regulation: Explaining Variation in the Governance of Deep Packet Inspection' (International Studies Annual Convention, New York City, 15-18 February 2009)

Bendrath Ralf and Mueller Milton, 'The End of the Net as We Know it? Deep Packet Inspection and Internet Governance' (2010) 13 New Media and Society 1142

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

Bennett Colin and others, 'Special Debate Section Discussing Bennett's Essay 'In Defense of Privacy'' (2011) 8 Surveillance & Society 485-516

Berglez Regina and Kreissl Reinhard, *Report on security enhancing options that are not based on surveillance technologies* (SurPRISE Project Deliverable D 3.3 2013)

Berramdane Abdelkhaleq, 'L'Ordre Public et les Droits Fondamentaux en Droit Communautaire et de l'Union Européenne' in authors Various (ed), *Territoires et liberté Mélanges en hommage au Doyen Yves Madiot* (Bruylant 2000)

Blair John, *The International Covenant on Civil and Political Rights and its (First) Optional Protocol. A short Commentary based on Views, General Comments and Concluding Observations by the Human Rights Committee* (Peter Lang 2005)

Bobbio Norberto, *L'Età dei Diritti* (Einaudi 1997)

Bobek Michal, 'Of Feasibility and Silent Elephants. The Legitimacy of the Court of Justice through the eyes of National Courts' in Adams Maurice and others (eds), *Judging Europe's Judges. The legitimacy of the case law of the European Court of Justice* (Hart Publishing 2013)

Braum Stefan, 'Are We Heading Towards a European form of 'Enemy Criminal Law'? On the Compatibility of Jakobs' Conception of 'an Enemy Criminal Law' and European Criminal Law' in Galli Francesca and Weyembergh Anne (eds), *EU counter-terrorism offences What impact on national legislation and case law?* (Editions de l'Université de Bruxelles 2012)

Brenner Susan, 'Is There Such a Thing as 'Virtual Crime'?' (2001) 4 California Criminal Law Review

——, 'The Council of Europe's Convention' in al. Jack M. Balkin et (ed), *Cybercrime, Digital Cops in a Networked Environment* (New York University Press 2007)

Brenner Susan and Koops Bert-Jaap (eds), *Cybercrime and Jurisdiction. A Global Survey* (TMC Asser Press 2006)

Brito Jerry and Watkins Tate, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy* (George Mason University 2011)

Brown Ian, 'Internet censorship: be careful what you ask for' (2008) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1026597>

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

Bygrave Lee A., *Data Privacy Law. An International Perspective* (Oxford University Press 2014)

Calderoni Francesco, 'The European Legal Framework on Cybercrime: Striving for an Effective Implementation' (2010) 54 Crime, Law and Social Change 339-357

Cameron Iain, *De Lege. National Security and the European Convention on Human Rights* (Iustus Förlag 2000)

Carrera Sergio and Guild Elspeth, *The European Council's Guidelines for the Area of Freedom, Security and Justice 2020: Subverting the 'Lisbonisation' of Justice and Home Affairs?* (CEPS Essay n° 13/14, 2014)

Cassese Antonio, *International Law (2nd edition)* (Oxford University Press 2005)

——, *I diritti umani oggi* (Laterza 2012)

Cayford Michelle, *Paper on Mass Surveillance by the National Security Agency (NSA) of the United States of America (*Extract from SURVEILLE Project Deliverable D 2.8 2014)

Cayford Michelle and others, *Consolidated Survey of Surveillance* Technologies (SURVEILLE Project Deliverable D 2.9 2015)

Ceccanti Stefano, 'L'antifascismo e le Nuove Costituzioni Democratiche' in De Bernardi Alberto and Ferrari Paolo (eds), *Antifascismo e Identità Europea* (Carocci 2004)

Chalmers Damian, 'Looking back at ERT and its contribution to an EU fundamental rights agenda' in Poiares Maduro Miguel and Azoulai Loïc (eds), *The Past and Future of EU Law. The Classics of EU Law Revisited on the 50th Anniversary of the Rome Treaty* (Hart Publishing 2010)

Chandler Jennifer A., 'The Autonomy of Technology: Do Courts Control Technology or Do They Just Legitimize its Social Acceptance?' (2007) 27 Bulletin of Science, Technology and Society 339-348

Christoffersen Jonas and Madsen Mikael Rask (eds), *The European Court of Human Rights between Law and Politics* (Oxford University Press 2011)

Christou George, *Cybersecurity in the European Union. Resilience and Adaptability in Governance and Policy* (Palgrave Macmillan 2015)

Clarke Roger, 'The Digital Persona and its Application to Surveillance' (1994) 10 The information society

——, 'The Legal Context of Privacy-Enhancing and Privacy-Sympathetic Technologies' (<http://www.rogerclarke.com/DV/Florham.html>, 1999)

——, 'Introducing PITs and PETs: Technologies Affecting Privacy' Privacy Law & Policy Reporter (http://www.rogerclarke.com/DV/PITsPETs.html, 2001)

——, 'Introduction to Information Security' (http://www.rogerclarke.com, 2001) accessed 1 September 2016

——, 'What's 'Privacy'? (<http://www.rogerclarke.com/DV/Privacy.html>, 2006)

——, *Deep Packet Inspection: its nature and implications* (<http://www.rogerclarke.com>, 2009)

——, 'PIA Origins and Development' (2009) 25 Computer Law & Security Review 123-135

Cocq Céline and Galli Francesca, *The use of surveillance technologies for the prevention and investigation of serious crimes (*SURVEILLE Project Deliverable D 4.1 2012)

Cohen Julie E., 'What Privacy is For' (2013) 126 Harvard Law Review 1094

Collier David, 'Understanding Process Tracing' (2011) 44 Political Science and Politics

Cotta Maurizio, Della Porta Donatella and Morlino Leonardo, *Scienza Politica* (Il Mulino 2001)

Coutts Stephen David, 'Union Citizenship and the Area of Freedom, Security and Justice' (PhD thesis, European University Institute 2015)

Craig Paul, *The Lisbon Treaty, Revised Edition: Law, Politics, and Treaty Reform* (Oxford University Press 2013)

Craig Paul and de Búrca Gráinne, *European Union Law: Text, Cases and Materials* (Oxford University Press, 2015)

Cremona Marise, *External Relations of the EU and the Member States: Competence, Mixed Agreements, International Responsibility, and Effects of International Law* (European University Institute Working Paper LAW 2006/22, 2006)

——, 'The EU and Global Emergencies: Competence and instruments' in Antoniadis Antonio, Schutze Robert and Spaventa Eleanor (eds), *The European Union and Global Emergencies: A Law and policy analysis* (Hart Publishing 2011)

—, 'Values in EU Foreign Policy' in Koutrakos Panos and Evans Malcoms (eds), *Beyond the Established Orders. Policy Interconnections between the EU and the Rest of the World* (Hart Publishing 2011)

—, 'The Two (or Three) Treaty Solution: The New Treaty Structure of the EU' in Biondi Andrea, Eeckhout Piet and Ripley Stephanie (eds), *European Union Law After the Treaty of Lisbon* (Oxford University Press 2012)

—, 'Who Can Make Treaties? The European Union' in Hollis Duncan (ed), *The Oxford Guide to Treaties* (Oxford University Press 2012)

—, 'A Triple Braid: Interactions between International Law, EU Law and Private Law' in Cremona Marise and Micklitz Hans-W (eds), *Private Law in the External Relation of the EU* (Oxford University Press 2016)

Cremona Marise, Francioni Francesco and Poli Sara, *Challenging the EU Counter-terrorism Measures through the Courts* (European University Institute Working Papers, Academy of European Law 2009/10, 2009)

Cremona Marise, Monar Joerg and Poli Sara (eds), *The External Dimension of the European Union's Area of Freedom, Security and Justice* (Peter Lang 2011)

Csikszentmihalyi Mihaly and Rochber-Halton Eugene, *The meaning of things. Domestic Symbols and the Self* (Cambridge University Press 1981)

Cunha Rodrigues José Narciso, 'The Incorporation of Fundamental Rights in the Community Legal Order' in Poiares Maduro Miguel and Azoulai Loïc (eds), *The Past and Future of EU Law. The Classics of EU Law Revisited on the 50th Anniversary of the Rome Treaty* (Hart Publishing 2010)

Curtin Deirdre, *Executive power in the European Union* (Oxford University Press 2009)

—, 'Overseeing Secrets in the EU: A Democratic Perspective' (2014) 52 Journal of Common Market Studies

Daly Angela, 'The Legality of Deep Packet Inspection' (First Interdisciplinary Workshop on Communications Policy and Regulation 'Communications and Competition Law and Policy – Challenges of the New Decade', University of Glasgow, 17 June 2010)

De Bernardi Alberto and Ferrari Paolo (eds), *Antifascismo e Identità Europea* (Carocci 2004)

de Búrca Gráinne, *The European Court of Justice and the International Legal Order after Kadi* (Jean Monnet Working Paper 01/09, New York University School of Law, 2009)

De Hert Paul, 'A Human Rights Perspective on Privacy and Data Protection Impact Assessments' in De Hert Paul and Wright David (eds), *Privacy Impact Assessment* (Springer 2012)

De Hert Paul and Gutwirth Serge, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Claes Erik, Gutwirth Serge and Duff Antony (eds), *Privacy and the criminal law* (Intersentia 2006)

—, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action' in Gutwirth Serge, Poullet Yves, De Hert Paul, Nouwt Sjaak and de Terwangne Cécile (ed), *Reinventing Data Protection?* (Springer 2009)

De Hert Paul and Wright David, *Privacy Impact Assessment* (Springer 2012)

De Rosa Mary, *Data Mining and Data Analysis for Counterterrorism* (Center for Strategic and International Studies, 2004)

Della Porta Donatella and Reiter Herbert, *Polizia e Protesta. L'Ordine Pubblico dalla Liberazione ai "no global"* (Il Mulino 2003)

Diffie Withfield and Susan Landau, 'Internet Eavesdropping: A Brave New World of Wiretapping' (2008) 299 Scientific American Magazine 4

Donohue Laura K., *The Cost of Counterterrorism. Power, Politics and Liberty* (Cambridge University Press 2008)

Drewer Daniel and Ellermann Jan, 'Europol's Data Protection Framework as an Asset in the Fight against Cybercrime' (Joint ERA-Europol conference Making Europe Safer: Europol at the Heart of European Security, The Hague, 18-19 June 2012)

Dumortier Frank and others, 'La Protection des Données dans l'Espace Européen de Liberté, de Sécurité et de Justice' 166 Journal de Droit Européen 23

Dunn Cavelty Maryam, 'National Security and the Internet: Distributed Security through Distributed Responsibility' in Giacomello Giampiero and Eriksson Johan (eds), *Who Controls the Internet? Beyond the Obstinacy or Obsolescence of the State*, vol 11 (International Studies Review 2009)

Dunn Cavelty Myriam, 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse' (2013) 15 International Studies Review 105

Dyzenhaus David, 'States of Emergency' in Rosenfeld Michel and Sajó András (eds), *The Oxford Handbook of Comparative Constitutional Law* (Oxford Handbooks Online 2012)

Edwards Lilian, Brown Ian and Marsden Christopher, 'Information Security and Cybercrime' in Edwards Lilian and Waelde Charlotte (eds), *Law and the Internet (3rd edition)* (Hart 2009) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1427776>

Edwards Lilian and Waelde Charlotte, *Law and the Internet* (Hart Publishing 2009)

Eriksson Johan and Giacomello Giampiero, 'Content Analysis in the Digital Age: Tools, Functions, and Implications for Security' in Gaycken Sandro and Krüger Jörg (ed), *The Secure Information Society: Ethical, Legal and Political Challenges* (Springer 2012)

Etzioni Amitai, *How Patriotic is the Patriot Act* (Routledge 2004)

Finn Rachel L., Wright David and Friedewald Michael, 'Seven Types of Privacy' in Gutwirth Serge, Leenes Ronald, De Hert Paul, and Poullet Yves (eds), *European Data Protection: Coming of Age* (Springer 2013) < http://works.bepress.com/michael_friedewald/60 >

Flanagan Anne, 'The Law and Computer Crime: Reading the Script of Reform' (2005) 13 International Journal of Law and Information Technology 98

Flanagan Anne and Walden Ian, 'Honeypots: a Sticky Legal Landscape?' (2009) 29 Rutgers Computer and Technology Law Journal 317

Fontaine André, *La Tache Rouge. Le Roman de la Guerre Froide* (Editions de la Martinière 2004)

Fried Charles, 'Privacy (a moral analysis)' in Schoeman Ferdinand David (ed), *Philosophical dimensions of privacy: an anthology* (Cambridge University Press 1984)

Fromm Eric, *Avere o Essere?* (Mondadori 1977)

Gajda Amy, *What If Samuel D. Warren Hadn't Married a Senator's Daughter?: Uncovering the Press Coverage That Led to the Right to Privacy* (Illinois Public Law and Legal Theory Research Papers Series, Research Paper n. 07-06, 2007)

Galli Francesca and Weyembergh Anne (eds), *EU Counter-terrorism Offences. What Impact on National Legislation and Case Law?* (Editions de l'Université de Bruxelles 2012)

Gavison Ruth, 'Privacy and the Limits of Law' in Schoeman Ferdinand David (ed), *Philosophical dimensions of privacy: an anthology* (Cambridge University Press 1984)

Gellman Robert, 'Fair Information Practices: A Basic History (Version 1.89)' (2012) Constantly updated at: <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>

Gercke Marco, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (International Telecommunication Union, Geneva, 2012)

Glendon Mary Ann, *The Transformation of Family Law. State, Law and Family in the United States and Western Europe* (The University of Chicago Press 1989)

González Fuster Gloria, 'Balancing Intellectual Property against Data Protection: a New Right's Wavering Weight' in Cerrillo i Martínez A. and others (eds), *Challenges and Opportunities of Online Entertainment. Proceedings of the 8th International Conference on Internet, Law & Politics Universitat Oberta de Catalunya* (UOC-Huygens Editorial 2012)

—, *The Emergence of Personal Data Protection as a Fundamental Right in Europe* (Springer 2014)

González Fuster Gloria and others, *Discussion Paper on Legal Approaches to Security, Privacy and Personal Data Protection (*PRISMS Project Deliverable D 5.1 2013)

Goodwin Morag, 'Chapter 1. Introduction. A Dimensions Approach to Technology Regulation' in Goodwin Morag, Koops Bert-Jaap and Leenes Ronald (eds), *Dimensions of Technology Regulation* (Wolf Legal Publishers (WLP) 2010)

Grabowski Mark, 'Are Technical Difficulties at the Supreme Court Causing a "Disregard of Duty"?' (2011) Journal of Law, Technology & Internet 93-112

Grief Nicholas, 'EU Law and Security' (2007) 32 European Law Review 752-765

Guelke John and others, *Matrix of Surveillance Technologies* (SURVEILLE Project Deliverable *D 2.6* 2013)

Hafner Katie and Lyon Matthew, *Where Wizards Stay up Late. The Origins of the Internet* (Free Press (pocket books) 2003)

Haggerty Kevin D. and Gazso Amber, 'Seeing Beyond the Ruins: Surveillance as a Response to Terrorist Threats' (2005) 30 Canadian Journal of Sociology 169-187

Hattery Angela J. and Smith Earl, 'Family' in Brunsma David L., Smith Keri Iyall and Gran Brian (eds), *The Handbook of Sociology and Human Rights* (Paradigm Publishers, Routledge 2013)

Herlin-Karnell Ester, 'EU Competence in Criminal Law after Lisbon' in Biondi Andrea, Piet Eeckhout and Ripley Stefanie (eds), *EU Law after Lisbon* (Oxford Scholarship Online 2012)

—, 'EU Values and the Shaping of the International Legal Context' in Amtenbrink Fabian and Kochenov Dimitri (eds), *European Union's Shaping of the International Legal Order* (Cambridge University Press 2013)

Herron Patrick, 'Beyond Balance: Targeted sanctions, security and republican freedom' in Orrù Elisa, Porcedda Maria Grazia and Volkmann Sebastian (eds), *Surveillance and control beyond the security v. privacy model* (Nomos Verlag forthcoming)

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

Hillion Christophe, 'Decentralised Integration? Fundamental Rights Protection in the EU Common Foreign and Security Policy' (2016) 1 European Papers - A Journal on Law and Integration

Hinarejos Alicia, 'Law and Order and Internal Security Provisions in the Area of Freedom, Security and Justice: Before and After Lisbon' in Eckes Christina and Konstadinides Theodore (eds), *Crime within the Area of Freedom, Security and Justice: a European Public Order* (2011)

Huysman Jef, *The Politics of Insecurity* (Routledge 2006)

Inness Julie C., *Privacy, Intimacy and Isolation* (Oxford Scholarship Online (2003) 1996)

Isenberg David, 'The Dawn of the 'Stupid Network'' (1998) 2 netWorker 24

Jacobs Francis G., 'The Lisbon Treaty and the Court of Justice' in Biondi Andrea, Eeckhout Piet and Ripley Stefanie (eds), *EU law after Lisbon* (Oxford Scholarship Online 2012)

Jenkins David, 'Introduction. The Long Decade' in Jenkins David, Jacobsen Amanda and Henrikens Anders (eds), *The long decade. How 9/11 changed the law* (Oxford University Press 2014)

Jouinia Mouna, Rabaia Latifa Ben Arfa and Aissab Anis Ben, 'Classification of Security Threats in Information Systems, 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014)' [2014] Procedia Computer Science 489 – 496

Jung Carl Gustav, *Tipi Psicologici* (Bollati Bornighieri 2011 (fifth edition))

Kaspersen Henrik, 'Jurisdiction in the Cybercrime Convention' in Koops Bert-Jaap and Brenner Susan (eds), *Cybercrime and jurisdiction. A global survey* (TMC Asser 2006)

Kertzer David I., 'Household History and Sociological Theory' (1991) 17 Annual Review of Sociology 155

Kilpatrick Claire, 'On the Rule of Law and Economic Emergency: the Degradation of Basic Legal Values in Europe's Bailouts' (2015) 35 Oxford Journal of Legal Studies p. 325

Kokott Juliane and Sobotta Christoph, 'The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' (2013) 3 International Data Privacy Law 222-228

Koops Bert-Jaap, 'Should ICT Regulation be Technology Neutral?' in Koops Bert-Jaap and others (eds), *Starting Points for ICT Regulation* (TMC Asser Press 2005)

—, 'The Trouble with European data Protection Law' (2014) 4 International Data Privacy Law 205-261

Kranenborg Herke, 'Access to Documents and Data Protection in European Union: on the Public Nature of Personal Data' (2008) 45 Common Market Law Review 1079-1114

Kreissl Reinhard and others, *Exploring the Challenges: Synthesis Report* (SurPRISE Project Deliverable D 3.4 2013)

Kshetri Nir, *The Global Cybercrime Industry. Economic, Institutional and Strategic Perspectives* (Springer 2010)

Kuehn Andreas and Mueller Milton, *Profiling the Profilers: Deep Packet Inspection for Behavioral Advertising in Europe and the United States* (Syracuse University, School of Information Studies, 2012)

Kulka Stefan and Zuiderveen Borgesius Frederik, 'Filtering for Copyright Enforcement in Europe after the Sabam Cases' (2012) 11 European Intellectual Property Review 54

Kuner Christopher and others, 'The Challenge of 'Big Data' for Data Protection' (2012) 2 International Data Privacy Law

Landau Susan, *Surveillance or Security? The Risk Posed by New Wiretapping Technologies* (the MIT Press 2010)

—, 'The Real Security Issues of the iPhone Case' (2016) 352 Science 1398-1399

Lanier Jaron, *Who Owns the Future?* (Penguin Books 2013)

Le Grand Guendal and Barrau Emilie, 'Prior Checking' in De Hert Paul and Wright David (eds), *Privacy Impact Assessment*, vol 6 (Springer 2012)

Leben Charles, 'Is there a EU Approach to Human Rights?' in Alston Philip, Bustelo Mara and Heenan James (eds), *The EU and Human Rights* (Oxford University Press 1999)

Leenes Ronald, 'Who Controls the Cloud?' (2010) 11 Revista de Internet, Derecho y Politica

—, 'Framing techno-regulation: an Exploration of State and Non-state Regulation by Technology' (2011) 5 Legisprudence

Lenaerts Koen, 'The Basic Constitutional Charter of a Community Based on the Rule of Law' in Poiares Maduro Miguel and Azoulai Loic (eds), *The Past and Future of EU Law. The Classics of EU Law Revisited on the 50th Anniversary of the Rome Treaty* (2010)

—, 'The Contribution of the European Court of Justice to the Area of Freedom, Security and Justice' (2010) 59 International and Comparative Law Quarterly 255

Levi Michael and Wall David S., 'Technology, Security and Privacy in Post-9/11 European Information Society' (2004) 31 Journal of Law and Society

Lipton Jacqueline, *Rethinking Cyberlaw. A new Vision for Internet Law* (Edwar Elgar Publishing 2015)

Lombarte Rallo Artemi, 'The Madrid Resolution and the prospect for a transnational PIAs' in De Hert Paul and Wright David (eds), *Privacy Impact Assessment*, vol 6 (Springer 2012)

Lynskey Orla, *The foundations of EU Data Protection Law* (Oxford University Press 2015)

Mankiw Gregory, *Principles of Economics (7th edition)* (Cengage Learning 2013)

Markatos Evangelos and Balzarotti Davide (eds), *The Red Book. A roadmap for systems security research* (The SysSec Consortium: A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: Europe for the World 2013)

Marsden Christopher, 'Internet Service Providers. Content, control and neutrality' in Walden Ian (ed), *Telecommunications law and regulation (4th edition)* (Oxford University Press 2012)

Mattioli Rossella, 'The 'State(s)' of cybersecurity' in Giacomello Giampiero (ed), *Security in Cyberspace* (Bloomsbury 2014)

McIntyre T. J., 'Child Abuse and Cleanfeeds: Assessing Internet Blocking Systems' in Brown Ian (ed), *Research Handbook on Governance of the Internet* (Edward Elgar 2013) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1893667>

Mendes Joana, *Rule of Law and Participation: A Normative Analysis of Internationalised Rulemaking as Composite Procedure* (Jean Monnet Working Paper Series, New York University School of Law, 2013)

Milward Alan, *European Rescue of the Nation State* (Taylor and Francis 1999)

Monahan Tony, *Surveillance and Security. Technological Politics and Power in Everyday Life* (Routledge 2006)

Monar Joerg, 'The Area of Freedom, Security and Justice' in von Bogdandy Armin and Bast Jürgen (eds), *Principles of European Constitutional Law* (Hart Publishing 2009)

Morsink Johannes, *The Universal Declaration of Human Rights: Origins, Drafting and Intent* (University of Pennsylvania Press 1999)

Moss Kate, *Balancing Liberty and Security. Human Rights, Human Wrongs* (Palgrave Macmillan 2011)

Mueller Milton, *DPI technology from the Standpoint of Internet Governance Studies: an Introduction (v1.1). The Network is Aware* (Syracuse University School of Information Studies, 2011)

Mueller Milton, Kuehn Andreas and Santoso Stephanie Michelle, 'Policing the Network: Using DPI for Copyright Enforcement' (2012) 9 Surveillance & Society 348

Mura Virgilio, *Categorie della Politica. Elementi per una teoria generale* (Giappichelli Editore 2004)

Murphy Robert F., 'Social Distance and the Veil' (1964) 66 American Anthropologist 1257-1274

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

Nissenbaum Helen, 'When Computer Security meets National Security' in Jack M. Balkin (ed), *Cybercrime, Digital Cops in a Networked Environment* (New York University Press 2007)

——, 'From Preemption to Circumvention: if Technology Regulates, why do we Need Regulation (and viceversa)?' (2011) 26 Berkeley Technology Law Journal 1367-1386

Nissenbaum Helen and Hansen Lene, 'Digital Disaster, Cyber Security, and the Copenhagen School' (2009) 53 International Studies Quarterly 1155

Northouse Clayton, *Protecting what matters. Technology, Security, and Liberty since 9/11* (Computer Ethics Institute, Brookings Institution Press 2006)

Nowak Manfred, 'Chapter on Article 17 ' in Nowak Manfred and Felix Ermacora (eds), *UN Covenant on Civil and Political Rights, CCPR Commentary (2nd edition)* (N.P. Engel 2005)

Ohm Paul, *The Rise and Fall of Invasive ISP Surveillance, Working Paper n. 8-22* (University of Colorado Law School 2008)

Ojanen Tuomas, 'Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance. Case Note on Court of Justice of the European Union, Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others' (2014) 10 European Constitutional Law Review 528–541

Orrù Elisa, 'Surveillance, Security and Legitimacy in the European Union' in Orrù Elisa, Porcedda Maria Grazia and Volkmann Sebastian (eds), *Surveillance and control beyond the security v. privacy model* (Nomos Verlag forthcoming)

Orrù Elisa, Porcedda Maria Grazia and Volkmann Sebastian (eds), *Surveillance and control beyond the security v. privacy model* (Nomos Verlag forthcoming)

Ottis Rain and Lorents Peeter, 'Cyberspace: Definitions and Implications' (Proceedings of the 5th International Conference on Information Warfare and Security, ICIW)

Parker David, '(Regulatory) Impact Assessment and Better Regulation' in Hert paul de and Wright David (eds), *Privacy Impact Assessment* (Springer 2012)

Pech Laurent, *The Rule of Law as a Constitutional Principle of the European Union* (Jean Monnet Working Paper Series, New York University School of Law, 2009)

——, *Rule of law as a Guiding Principle of the European Union's External Action* (CLEER Working Papers, Centre for the Law of EU External Relations, TMC Asser Instituut Inter-university Research Centre, 2013)

Peers Steve, *EU Justice and Home Affairs Law* (Oxford University Press 2011)

Peter Swire and Lauren Steinfeld, 'Security and Privacy After September 11: The Health Care Example' 86 Minnesota Law Review

Piris Jean-Claude, *The Lisbon Treaty. A Legal and Political Analysis* (Cambridge 2010)

Poli Sara and Tzanou Maria, 'The Kadi Rulings: A Survey of the Literature' in Cremona Marise, Francioni Francesco and Poli Sara (eds), *Challenging the EU Counter-terrorism Measures through the Courts* (European University Institute, AEL Working Paper 10, 2009)

Porcedda Maria Grazia, 'Data Protection and the Prevention of Cybercrime: a dual role for security policy in the EU?' (LL.M. thesis, European University Institute 2011)

——, *Data Protection and the Prevention of Cybercrime: the EU as an Area of Security?* (European University Institute Working Paper, Law 2012/25, 2012)

——, 'Reviving Privacy: the Opportunity of Cybersecurity' in *Challenges and Opportunities of Online Entertainment. Proceedings of the 8th International Conference on Internet, Law & Politics Universitat Oberta de Catalunya* (UOC-Huygens Editorial 2012)

——, 'Lessons from PRISM and Tempora: the Self-contradictory Nature of the Fight against Cyberspace Crimes. Deep Packet Inspection as a Case Study' (2013) 25 Neue Kriminalpolitik 305-409

——, *Paper Establishing Classification of Technologies on the Basis of their Intrusiveness into Fundamental Rights* (SURVEILLE Project Deliverable D 2.4, European University Institute 2013)

——, 'Public-Private Partnerships: A 'Soft' Approach to Cybersecurity? Views from the European Union' in Giacomello Giampiero (ed), *Security in Cyberspace: Targeting Nations, Infrastructures, Individuals* (Continuum Books, Bloomsbury Publishing 2014)

——, 'Rule of Law and Human Rights in Cyberspace' in Pawlak Patryk (ed), *Riding the Digital Wave – The impact of cyber capacity building on human development, Report n. 21* (European Union Institute of Security Studies 2014)

——, 'The Manifold Significance of Citizens' Legal Recommendations on Privacy, Security and Surveillance' in Friedewald Michael, Burgess J. Peter, Čas Johann, Bellanova Rocco and Peissl Walter (eds), *Surveillance, Privacy and Security. Citizens' Perspectives* (Routledge 2017)

——, 'The Recrudescence of 'Security v. Privacy' after the 2015 Terrorist Attacks, and the Value of 'Privacy Rights' in the European Union' in Orrù Elisa, Porcedda Maria Grazia and

Volkmann Sebastian (eds), *Surveillance and control beyond the security v. privacy model* (Nomos Verlag forthcoming)

Porcedda Maria Grazia, Vermeulen Mathias and Scheinin Martin, *Report on Regulatory Frameworks Concerning Privacy and the Evolution of the Norm of the Right to Privacy* (SurPRISE Project Deliverable D 3.2, European University Institute 2013)

Poscher Ralf and Miller Russell, 'Surveillance and Data Protection in the Conflict between European and American Legal Cultures' (<http://www.aicgs.org/issue/surveillance-and-data-protection-in-the-conflict-between-european-and-american-legal-cultures/> 2013)

Posner Eric and Vermeule Adrian, *Terror in the balance. Security, liberty and the courts* (Oxford University Press 2007)

Poullet Yves and Rouvroy Antoinette, 'The Right to Informational Self-determination and the Value of Self-development. Reassessing the Importance of Privacy for Democracy' in Gutwirth Serge and others (eds), *Reinventing Data Protection?* (2009) <http://works.bepress.com/antoinette_rouvroy/7 >

Prosser William, 'Privacy' (1960) 48 California law review 383-423

Pugliese Giovanni, 'Appunti per una Storia della Protezione dei Diritti Umani' (1989) 43 Rivista trimestrale di diritto e procedura civile 619-659

Puschmann Paul and Solli Arne, 'Household and Family during Urbanization and Industrialization: Efforts to Shed New Light on an Old Debate' (2014) 19 The History of the Family 1

Raab Charles and Wright David, 'Surveillance: Extending the Limits of Privacy Impact Assessments' in De Hert Paul and Wright David (eds), *Privacy Impact Assessment*, vol 6 (Springer 2012)

Rapone Leonardo, *Storia dell'Integrazione Europea* (Carocci 2004)

Rapoport Michele, 'Domestic Surveillance Technologies and a New Visibility' in Orrù Elisa, Porcedda Maria Grazia and Volkmann Sebastian (eds), *Surveillance and control beyond the security v. privacy model* (Nomos Verlag forthcoming)

Reed Chris, 'Taking Sides on Technology Neutrality' (2007) 4 Script-ed

Regan Priscilla, 'Privacy as a Common Good in the Digital World' (2002) 5 Information, Communication & Society 382–405

Rehof Lars Adam, 'The Universal Declaration of Human Rights: A Commentary' in Eide Asbjorn, Alfredsson Gudmundur, Melander Goran, Rehof Lars Adam and Rosas Allan, with the collaboration of Swinehart Teresa (eds.), (Scandinavian University Press 1992)

——, 'Universal Declaration of Human Rights – Common Standard of Achievement' in Eide Asbjorn and Alfredsson Gudmundur (eds), (Scandinavian University Press 1995)

Reiman Jeffrey H., 'Privacy, Intimacy and Personhood' in Schoeman Ferdinand David (ed), *Philosophical dimensions of privacy: an anthology* (Cambridge University Press 1984)

——, 'Driving to the Panopticon: Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future (Symposium Paper)' (1995) 11 Santa Clara Computer and High Technology Law Journal 27

Rodotà Stefano, *Elaboratori Elettronici e Controllo Sociale* (Mulino 1973)

——, *Intervista su Privacy e Libertà. A cura di Paolo Conti* (2005)

——, ‘Data Protection as a Fundamental Right’ in Gutwirth Serge, Poullet Yves, De Hert Paul, Nouwt Sjaak and de Terwangne Cécile (eds), *In Reinventing Data Protection?* (Springer 2009)

——, *Il diritto di avere diritti* (Editori Laterza 2012)

——, *Il Mondo nella Rete. Quali i Diritti, Quali i Vincoli* (Editori Laterza 2014)

Romero Federico, ‘Antifascismo e Ordine Internazionale’ in De Bernardi Alberto and Ferrari Paolo (eds), *Antifascismo e Identità Europea* (Carocci 2004)

Rosas Allan and Armati Lorna, *EU Constitutional Law - An Introduction* (Hart Publishing 2010)

Savin Andrej, *EU Internet Law* (Elgar 2013)

Scheinin Martin, ‘Characteristics of Human Rights Norms’ in Krause Catarina and Scheinin Martin (eds), *International Protection of Human Rights: a Textbook* (Abo Akademi Institute for Human Rights 2009)

——, *Terrorism and the Pull of ‘Balancing’ in the Name of Security. Law and Security, Facing the Dilemmas* (European University Institute Law Working Paper 11, 2009)

——, *Written testimony related to the surveillance program conducted under Section 702 of the FISA Amendments Act* (2014)

Scheinin Martin and others, *Annex 3 to SURVEILLE Project deliverable 2.6 (matrix of surveillance technologies): fundamental rights technology assessment sheets (EUI)* (2013)

Scheinin Martin and Sorell Tom, *Synthesis Report from WP4, merging the ethics and law analysis and discussing their outcomes* (SURVEILLE Project Deliverable D 2.10 2015)

Scheinin Martin and Vermeulen Mathias, ‘Unilateral Exceptions to International Law: Systematic Legal Analysis and Critique of Doctrines to Deny or Reduce the Applicability of Human Rights Norms in the Fight against Terrorism’ (2011) 8 Essex Human Rights Review 20-56

Schoeman Ferdinand David, *Philosophical Dimensions of Privacy: an Anthology* (Cambridge University Press 1984)

Schullhofer Stephen J., *Rethinking the Patriot Act. Keeping America Safe and Free* (A Century Foundation Report, 2005)

Simitis Spiros, *Revisiting sensitive data* (Council of Europe, 1999)

——, ‘Privacy - An Endless Debate’ (2010) 98 California law review

Solove Daniel, ‘"I’ve Got Nothing to Hide" and Other Misunderstandings of Privacy’ (2007) 44 San Diego Law Review 745

——, *Nothing to Hide: the False Tradeoff Between Privacy and Security* (Yale University Press 2011)

Sommer Peter and Brown Ian, *Reducing Systemic Cybersecurity Risks* (OECD/IFP Project on Future Global Shocks, IFP/WKP/FGS(2011)3 2011)

Spaventa Eleanor, ‘Counter-Terrorism and Fundamental Rights: Judicial Challenges and Legislative Changes after the Rulings in Kadi and PMOI’ in Antoniadis Antonio, Schutze Robert and Spaventa Eleanor (eds), *The European Union and Global Emergencies: A Law and policy analysis* (Hart Publishing 2011)

Sugman Stubbs Katija and Galli Francesca, ‘Inchoate Offences.The Sanctioning of an Act Prior to and Irrespective of the Commission of any Harm’ in Galli Francesca and Weyembergh

Anne (eds), *EU counter-terrorism offences. What impact on national legislation and case law?* (Editions de l'Université de Bruxelles 2012)

SURVEILLE Project Consortium, *Description of Works of the SURVEILLE Project. Surveillance: ethical issues, legal limitations and efficiency* (Seventh Framework Programme, European Union 2011)

Swire Peter, 'A Model for When Disclosure Helps Security: What is Different about Computer and Network Security?' (2004) 2 Journal on Telecommunications and High Technology Law

Tanenbaum Andrew S. and Wetherall David J., *Reti di Calcolatori (Quinta Edizione)* (Pearson Italia 2011)

Taylor Charles, *Sources of the Self. The Making of the Modern Identity* (Cambridge University Press 1989)

——, *The Ethics of Authenticity* (Harvard University Press 1992)

Tene Omer and Polonetsky Jules, 'Privacy in the Age of Big Data: A Time for Big Decisions' (2012) 64 Stanford Law Review Online

Tien Lee, 'Architectural Regulation and the Future of Social Norms' in in Jack M. Balkin (ed), *Cybercrime, Digital Cops in a Networked Environment* (New York University Press 2007)

Timmermans Christiaan, 'The Specificity of Private Law in EU External Relations: The Area of Freedom, Security, and Justice' in Cremona Marise and Micklitz Hans-W (eds), *Private Law in the External Relations of the EU* (Oxford University Press 2016)

Tridimas Takis, *The General Principles of EU Law* (Oxford University Press 2006)

——, 'Primacy, Fundamental Rights and the Search for Legitimacy' in Poiares Maduro Miguel and Azoulai Loïc (eds), *The Past and Future of EU Law. The Classics of EU Law Revisited on the 50th Anniversary of the Rome Treaty* (Hart Publishing 2010)

Tzanou Maria, 'EU Counter-terrorism Measures and the Question of Fundamental Rights: The Case of Personal Data Protection' (PhD thesis, European University Institute 2012)

Unabhaengiges Landeszentrum fuer Datenschutz (ULD), *Report on Surveillance Technology and Privacy Enhancing Design* (SurPRISE Project Deliverable D 3.1, 2013)

Van Schewick Barbara, *Internet Architecture and Innovation* (MIT press 2010)

Vermeule Adrian, 'Critiques of the Trade-off Thesis' in Jenkins David, Jacobsen Amanda and Henrikens Anders (eds), *The Long Decade. How 9/11 Changed the Law* (Oxford University Press 2014)

Viola de Azevedo Cunha Mario, 'The Concept of Personal Data in the Post Lisbon Era: is there Need (and room) for Change?' in Gutwirth Serge and others (eds), *Data Protection in Good Health?* (Springer 2012)

Von Bogdandy Armin, 'Founding Principles of EU Law: A Theoretical and Doctrinal Sketch' (2010) 16 European Law Journal

Walden Ian (ed), *Telecommunications Law and Regulation (4th edition)* (Oxford University Press 2012)

Waldron Jeremy, 'The Concept and the Rule of Law' (2008) 43 Georgia Law Review 1

——, *Torture, Terrore and Trade-offs. Philosophy for the White House* (Oxford University Press 2010)

Ward Peter, *A History of Domestic Space: Privacy and the Canadian Home* (University of British Columbia press 1999)

Warren Samuel D. and Brandeis Louis D., 'The Right to Privacy' (1980) 4 Harvard Law Review

Weber Max, *La Scienza come Professione. La Politica come Professione* (Einaudi 2004)

Weiler Joseph H. H., 'Epilogue: Judging the Judges - Apology and Critique' in Adams Maurice and others (eds), *Judging Europe's Judges. The legitimacy of the case law of the European Court of Justice* (Hart Publishing 2013)

Wertheim Margaret, *The Pearly Gates of Cybersapce. A History of Space from Dante to the Internet* (W. W. Norton & Company Inc. 1999)

Westin Alan, *Privacy and Freedom* (Atheneum Press 1967)

Wright David and others, 'Minimizing Technology Risks with PIAs, Precaution, and Participation' (2011) 30 IEEE Technology and Society Magazine 47

Wright David and others, *A Privacy Impact Assessment Framework for Data Protection and Privacy Rights* (*PIAF Project Deliverable D.1* Report Prepared for the European Commission, Directorate General Justice, 2011)

Wuyts Kim, *LINDDUN: a privacy threat analysis framework*

Wyuts Kim, Scandariato Riccardo and Joosen Wouter, *LIND(D)UN Privacy Threat Tree Catalog* (Report CW 675, KU Leuven, 2014)

Zalnieriute Monika, 'Towards International Data Privacy Cooperation: Strategies and Alternatives' (PhD thesis, European University Institute 2014)

Zeno-Zencovich Vincenzo, 'Articolo 8. Diritto al Rispetto della Vita Privata e Familiare' in Sergio Bartole Benedetto Conforti e Guido Raimondi (ed), *Commentario alla Convenzione Europea per la Tutela dei Diritti dell'Uomo e delle Libertà Fondamentali* (Cedam 2001)

Zittrain Jonathan, *The Future of the Internet and How to Stop it* (Yale University Press 2008)

2.2 POLICY DOCUMENTS

2.2.1 EU POLICY DOCUMENTS

Article 29 Data Protection Working Party, *Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive (Working Document),* (DG XV D/5025/98 WP 12, 1998)

—, *Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance* (11750/02/EN WP 89, 2004)

—, *Opinion 2/2006 on Privacy Issues related to the Provision of Email Screening Services* (00451/06/EN WP 118, 2006)

—, *Opinion 4/2007 on the Concept of Personal Data* (01248/07/EN WP 136, 2007)

—, *Opinion 15/2011 on the Definition of Consent* (01197/11/EN WP 187, 2011)

—, *Opinion 03/2013 on Purpose Limitation* (00569/13/EN WP 203, 2013)

—, *Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector* (536/14/EN WP 211, 2014)

—, *Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes* (819/14/EN WP 215, 2014)

—, *Opinion 05/2014 on Anonymisation Techniques* (0829/14/EN WP216, 2014)

——, *Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks* (14/EN WP 218, 2014)

——, and 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, 2009)

Bangemann Martin and al. et, *The 'Recommendations to the European Council. Europe and the global information society'. The Bangemann Report* (1994)

Body of European Regulators for Electronic Communications (BEREC), *A Framework for Quality of Service in the scope of Net Neutrality* (BoR (11) 53, 2011)

——, *BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules* (BoR (16) 127, 2016)

Committee of Ministers of the Council of Europe, *The Council of Europe and the Rule of Law - An overview, CM (2008) 170 (CoE and the Rule of Law)* (2008)

——, *Reply of the Committee of Ministers to Parliamentary Assembly Recommendation 2067 (2015) on Mass Surveillance* (CM/AS(2015)Rec2067-final, 2015)

Council, *The Stockholm Programme. An Open and Secure Europe Serving and Protecting Citizens, OJ C 115* (2010)

——, *Draft Internal Security Strategy for the European Union: Towards a European Security Model, 5842/2/10* (2010)

——, *EU Cyber Defence Policy Framework, 15585/14* (2014)

——, *Draft Annex Conclusions on the Renewed European Internal Security Strategy 2015-2020, 9797/15* (2015)

Conclusions of the Council of the EU and of the Member States meeting within the Council on Counter-Terrorism, n° 848/15 (Council 2015)

Dati Rachida, (Rapporteur), *Draft Report on prevention of radicalisation and recruitment of European citizens by terrorist organisations (2015/2063(INI))* (European Parliament, Committee on Civil Liberties, Justice and Home Affairs, 2015)

European Commission, *Directive Concerning The Protection of Individuals in Relation to the Processing of Personal Data, Recommendation for a Council Decision on the Opening of Negotiations With a View to the Accession of the European Communities to the Council of Europe Convention for the Protection of Individuals With Regard to the Automatic Processing of Personal Data, Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security* ((Communication) COM (90) 314 final, 1990)

——, *White Paper on Growth, Competitiveness, Employment. The Challenges and Ways forward into the 21st Century* ((Communication) COM (93) 700, 1993)

——, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime* ((Communication) COM (2000) 890 final, 2000)

——, *Network and Information Security: Proposal for a European Policy Approach* ((Communication) COM (2001) 298, 2001)

—, *Compliance with the Charter of Fundamental Rights in Commission legislative proposals. Methodology for systematic and rigorous monitoring* ((Communication) COM (2005) 172 final, 2005)

—, *Promoting Data Protection by Privacy Enhancing Technologies (PETs)* ((Communication) COM (2007) 228 final, 2007)

—, *Critical information infrastructure protection. Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience* ((Communication) COM (2009) 149 final, 2009)

—, *Report on the Practical Operation of the Methodology for a Systematic and Rigorous Monitoring of Compliance with the Charter of Fundamental Rights* ((Communication) COM (2009) 205 final, 2009)

—, *A Comprehensive Approach on Personal Data Protection in the European Union* ((Communication) COM (2010) 609 final, 2010)

—, *Delivering an Area of Freedom, Security and Justice for Europe's citizens – Action Plan Implementing the Stockholm Programme* ((Communication) COM (2010) 171 final, 2010)

—, *Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union* ((Communication) COM (2010) 573/4, 2010)

—, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (General Data Protection Regulation)* ((Communication) COM (2012) 11 final, 2012)

—, *Annexes to the Communication 'A new EU Framework to strengthen the Rule of Law'* ((Communication) COM (2014) 158 final, 2014)

—, *A New EU Framework to Strengthen the Rule of Law* ((Communication) COM (2014) 158 final, 2014)

—, *An Open and Secure Europe: Making it Happen* ((Communication) COM (2014) 154 final {SWD(2014) 63 final}, 2014)

—, *A Digital Single Market Strategy for Europe* ((Communication) COM (2015) 192 final, 2015)

—, *The European Agenda on Security* ((Communication) COM(2015) 185 final, 2015)

—, *Proposal for a Directive on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism* ((Communication) COM (2015) 625 final, 2015)

—, *Commission Decision of 5 July 2016 on the Signing of a Contractual Arrangement on a Public-private Partnership for Cybersecurity Industrial Research and Innovation between the European Union, Represented by the Commission, and the Stakeholder Organisation,* (C(2016) 4400 final, 2016)

—, *Contractual Public Private Partnership on Cybersecurity & Accompanying Measures. Accompanying the document Commission Decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research "an innovation between the European Union, represented by the Commision, and the stakeholder organisation"* (Staff Working Document) SWD (2016) 216 final, 2016)

——, *Delivering on the European Agenda on Security to Fight against Terrorism and Pave the Way towards an Effective and Genuine Security Union* ((Communication) COM (2016) 230 final, 2016)

——, *Proposal for a Directive Establishing the European Electronic Communications Code* ((Communication) COM(2016) 590 final, 2016/0288 (COD), 2016)

——, *Proposal for a Directive of the European Parliament and of Council on Certain Permitted Uses of Works and Other Subject-matter Protected by Copyright and Related Rights for the Benefit of Persons who are Blind, Visually Impaired or Otherwise Print Disabled and Amending Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society* ((Communication) COM(2016)0596 final, 2016)

——, *Strengthening Europe's Cyber Resilience System* ((Communication) COM(2016) 640 final, 2016)

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, *Cyber Security Strategy: An Open, Safe and Secure Cyberspace* ((Joint Communication) JOIN (2013) 01 final, 2013)

——, *Joint Framework on countering hybrid threats. A European Union response* ((Joint Communication) JOIN (2016) 18 final, 2016)

European Council, *Report on the Implementation of the European Security Strategy – Providing Security in a Changing World* ((European Security Strategy) S407/08, 2008)

European Data Protection Supervisor, *Developing a 'Toolkit' for Assessing the Necessity of Measures that Interfere with Fundamental Rights* (Background Paper for Consultation, 2016)

——, *Opinion on Net Neutrality, Traffic Management and the Protection of Privacy and Personal Data* (OJ C 34, p 1–17, 2011)

European Group on Ethics in Science and New Technologies, *Ethics of Security and Surveillance Technologies. Opinion n. 28* (2014)

European Network and Information Security Agency (ENISA), *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools* (2006)

European Council, Conclusions, 26/27 June 2014, EUCO 79/14 (2014)

European Parliament, 'Interception Capabilities 2014' (2014) <http://www.europarl.europa.eu/document/activities/cont/201309/20130916ATT71388/20130916ATT71388EN.pdf>

——, *LIBE Committee Inquiry on the Electronic Mass Surveillance of EU Citizens: Protecting fundamental Rights in a Digital Age. Proceedings, Outcome and Background Documents* (2014)

——, *Resolution on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs* (2013/2188 (INI), 2014)

——, LIBE Committee, *Statement by Professor Martin Scheinin* (Hearing within the Inquiry on Electronic Mass Surveillance of EU Citizens, 2013)

——, LIBE Secretariat, *Background Note. The European Parliament's temporary committee on the ECHELON interception system* (2014)

—, Mady Delvaux (Rapporteur), *Draft Report with Recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103 (INL), 2016)

European Union Network of Independent Experts on Fundamental Rights, *Commentary of the Charter of Fundamental Rights of The European Union* (<http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf> 2006)

Fundamental Rights Agency, *Using indicators to measure fundamental rights in the EU: challenges and solutions* (2nd Annual FRA Symposium Report, 2001)

—, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Mapping Member States' legal frameworks* (Publications Office of the European Union, 2015)

—, *Ensuring Justice for Hate Crime Victims: Professional Perspectives* (2016)

Juncker Jean-Claude, *Council of Europe – European Union: a sole Ambition for the European Continent* (Report to the Attention of Heads of State or Government of the Member States of Council of Europe, 2006)

Marinos Louis, Belmonte Adrian and Rekleitis Evangelos, *ENISA Threat Landscape 2015* (European Network and Information Security Agency (ENISA), 2016)

2.2.2 CoE Policy documents

Council of Europe, Division de la Recherche de la Cour Européenne des Droits de l'Homme, *Sécurité nationale et Jurisprudence de la Cour Européenne des Droits de l'Homme* (Council of Europe, 2013)

Council of Europe, Parliamentary Assembly, *Recommendation 2067 (2015) on Mass Surveillance* (2015)

— *Resolution 2045 (2015) on Mass Surveillance* (2015)

Council of Europe, Venice Commission, *Report on the Rule of Law* (Study No 512/2009, 2011)

—, *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on Democratic Oversight of Signals Intelligence Agencies* (CDL-AD(2015)006, Study N 719/2013, 2015)

2.2.3 UN Policy documents

International Telecommunication Union, *Security in Telecommunications and Information Technology. An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications* (ITU, Geneva, 2015)

International Telecommunication Union (ITU-T), *Requirements for deep packet inspection in next generation networks, Recommendation ITU-T Y.2770* (2012)

Scheinin Martin, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, A/HRC/13/37* (2009)

United Nations, *Report of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174* (2015)

—, Development Programme (UNDP), *Human Develpoment Report* (Oxford University Press, 1994)

—, High Commissioner for Human Rights (OHCHR), *Human Rights Indicators. A Guide to Measurement and Implementation* (HR/PUB/12/5, 2012)

—, International Human Rights Instruments, *Report on Indicators for Monitoring Compliance with International Human Rights Instruments* (HRI/MC/2006/7, 2006)

—, Office for Disarmament Affairs, 'Developments in the Field of Information and Telecommunications in the Context of International Security' <https://www.un.org/disarmament/topics/informationsecurity/> accessed 26 September 2016

—, Office on Drug and Crime (UNODC), *The Use of Internet for Terrorist Purposes* (2012)

United Nations, Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (UNODC/CCPCJ/EG4/2013/3, 2013)

—, Secretary General, *The Rule of Law and Transitional Justice in Conflict and Post-conflict Societies. Report of the Secretary-General to the Security Council* (S/2004/616, 2004)

2.2.4 OTHER POLICY DOCUMENTS AND STUDIES

Akdeniz Yaman, *Report. Freedom of Expression on the Internet. A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States* (2011)

Amnesty International, *Des Vies bouleversées. L'Impact Disproportionné de l'Etat d'Urgence en France* (Londres, 2016)

—, and International Commission of Jurists Open Society Foundations, *Joint Statement: After a Fast-track Process the European Parliament Takes a Troubling Position on Counter-terrorism in Europe* (2016)

Anderson David, *The Terrorism Acts in 2011. Report of the Independent Reviewer on the Operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006* (Parliament, The Stationery Office 2012)

Bonfanti Matteo, González Fuster Gloria and Porcedda Maria Grazia, 'European Union' in Privacy International (ed), *Global Surveillance Monitor* (2011)

Candler Jean and others, *Human Rights Measurement Framework: Prototype panels, indicator set and evidence base* (Equality and Human Rights Commission 2011)

Cavoukian Ann, *Privacy by Design in Law, Policy and Practice. A White Paper for Regulators, Decision-makers and Policy-makers* (Information and Privacy Commissioner, Ontario 2011)

Congreso de los Diputados, *Comisiones de Investigacíon sobre el 11 de marzo de 2004, Diario de Sesiones n° 24* (Cortes Generales, 2005)

Danezis George and others, *Privacy and Data Protection by Design – from Policy to Engineering* (ENISA 2014)

Del Sesto Ronald W., Jr., and Frankel Jon, 'How Deep Packet Inspection Changed the Privacy Debate' (Office of the Information & Privacy Commissioner of Ontario, Canada, 2008 previously at: <http://dpi.priv.gc.ca/>)

Dragicevic Drazen, Henrik Kaspersen and Joseph Sherwa, *Conditions and Safeguards under the Budapest Convention on Cybercrime, Discussion Paper, EU/COE Joint Project on Regional Cooperation against Cybercrime* (Council of Europe 2012)

Fenech M. George and Pietrasanta M. Sébastien, *Rapport fait au Nom de la Commission d'Enquete Relative aux Moyens mis en œuvre par l'État pour Lutter Contre le Terrorisme Depuis le 7 janvier 2015* (Assemblé Nationale, 2016)

Gayrel Claire and others, *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 2010)

Global Alliance Partners, *Guiding principles on the Global Alliance against child sexual abuse online. Annex to the Declaration on Launching the Global Alliance against child sexual abuse online* (2012)

Hülsmann Werner, Irion Kristina and Laurant Cédric, 'Germany' in Privacy International (ed), *Global Surveillance Monitor* (2011)

Human Rights Watch, *France: Abus Commis dans le Cadre de l'Etat d'Urgence. Les Perquisitions Administratives et les Assignations à Résidence sans Autorisation Judiciaire Doivent Cesser* (3 February, 2016)

International Conference of Data Protection and Privacy Commissioners, *Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data (The Madrid Resolution)* (30th International Conference of Data Protection and Privacy Commissioners 2009)

Jeselon Pat and Fineberg Anita, *A Foundational Framework for a Privacy by Design Privacy Impact Assessment* (Office of the Information & Privacy Commissioner of Ontario, Canada 2011)

Ministère de l'Intérieur français, *Initiative Franco-allemande sur la Sécurité Intérieure en Europe* (Retrieved on EDRi-gram newsletter 14.16, 24 August 2016)

OECD, Development Assistance Committee (DAC), *Security System Reform and Governance* (DAC Guidelines and Reference Series, 2005)

United Kingdom, Home Office, *Report of the Official Account of the Bombings in London on 7th July 2005* (House of Commons, 2006)

United Kingdom, House of Lords, *Personal Internet Security* (Science and Technology Committee, 5th Report of Session 2006-07 edn, 2007)

——, *Surveillance: Citizens and the State* (House of Lords Select Committee on the Constitution, 2009)

White House, *President's Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (2009)

——, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World* (2011)

2.3 NEWSPAPER ARTICLES

'Hollande Mantient sa Position: "La France est en Guerre"' *Le Monde* (16 November 2015) <http://www.lemonde.fr/attaques-a-paris/video/2015/11/16/hollande-maintient-sa-position-la-france-est-en-guerre_4811152_4809495.html>

Atran Scott and Hamid Nafees, 'Paris: the War Isis Wants' *The New York Review of Books* (16 November 2015) <http://www.nybooks.com/daily/2015/11/16/paris-attacks-isis-strategy-chaos/>

Bekmezian Hélène, 'L'Etat d'Urgence Prolongé pour Six Mois par l'Assemblée Nationale' *Le Monde* (Paris, 19 July 2016) <http://www.lemonde.fr/politique/article/2016/07/19/etat-d-urgence-le-gouvernement-se-veut-ouvert-aux-propositions-de-la-droite_4971808_823448.html>

Bonnefous Bastien and Wieder Thomas, 'Hollande Confirme la Déchéance de Nationalité' *Le Monde* (Paris, 2 January 2016)

Dodd Vikram and Gayle Damien, 'Police to Hire Law Firms to Tackle Cyber Criminals in Radical Pilot Project' *The Guardian* (14 August 2016) <https://www.theguardian.com/uk-news/2016/aug/14/police-to-hire-law-firms-to-tackle-cyber-criminals-in-radical-pilot-project?CMP=share_btn_link>

Donohue Laura K., 'NSA Surveillance May Be Legal — but it's Unconstitutional' *The Washington Post* (21 June 2013)

Fung Brian, 'The Aereo Case is Being Decided by People who Call iCloud 'the iCloud.' Yes, Really' *The Washington Post* (13 April 2014) <https://www.washingtonpost.com/news/the-switch/wp/2014/04/23/the-aereo-case-is-being-decided-by-people-who-call-icloud-the-icloud-yes-really/>

Gellman Barton and Poitras Laura, 'Documents: U.S. Mining Data from 9 Leading Internet Firms; Companies Deny Knowledge' *Washington Post* (6 June 2013)

Ghume Sunil, 'Senior Officers don't Even Look at Intelligence Reports: 26/11 Panel' *The Times of India* (2 December) <http://timesofindia.indiatimes.com/india/Senior-officers-dont-even-look-at-intelligence-reports-26/11-panel/articleshow/5289956.cms?referral=PM>

Goodin Dan, 'Police Body Cams Found Pre-installed with Notorious Conficker Worm' *ArsTechnica.com* (16 November 2015) <http://arstechnica.com/security/2015/11/police-body-cams-found-pre-installed-with-notorious-conficker-worm/>

Greenberg Andy, 'The Shadow Broker Mess is What Happens When the NSA Hoards Zero-days' *Wired* (17 August 2016) <https://www.wired.com/2016/08/shadow-brokers-mess-happens-nsa-hoards-zero-days/>

Greenwald Glenn and Ball James, 'Revealed: the Top Secret Rules that Allow NSA to Use US Data without a Warrant' *The Guardian* (20 June 2013)

Greenwald Glenn and MacAskill Ewen, 'NSA Taps in to Systems of Google, Facebook, Apple and Others, Secret Files Reveal' *The Guardian* (7 June 2013)

Iannaccone Sandro, 'Cybersicurezza, Attenti alle Tastiere Wireless' *La Repubblica* <http://www.repubblica.it/tecnologia/2016/08/29/news/cybersicurezza_attenti_alle_tastiere_wireless-146770289/> accessed 1 September 2016

Jacquin Jean-Baptiste, 'L'impossible Sortie de l'Etat d'Urgence' *Le Monde* (Paris, 2 January 2016)

Kahn David, ‘Back When Spies Played by the Rules’ *The New York Times* (13 January 2006) <http://www.nytimes.com/2006/01/13/opinion/13kahn.html?_r=0>

Kravets David, ‘Internet Tracking Software Maker to Face Wiretapping Trial, Court Rules’ *ArsTechnica.com* (17 August 2016) <http://arstechnica.com/tech-policy/2016/08/internet-tracking-software-maker-to-face-wiretapping-trial-court-rules/>

Lepore Jill, ‘The PRISM. Privacy in an Age of Publicity’ *The New Yorker* (24 June 2013)

Lillington Karlin, ‘It’s Good to Talk in Public about Privacy and Data Protection’ *Irishtimes.com* (19 June 2013)

MacAskill Ewen and others, ‘GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications’ *The Guardian* (21 June 2013)

Menn Jospeh, ‘Exclusive: Yahoo Secretly Scanned Customer Emails for U.S. Intelligence Sources’ (4 November 2016) <http://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT>

Mullin Joe, ‘Privacy Lawsuit over Gmail Will Move Forward’ (16 August 2016) <http://arstechnica.com/tech-policy/2016/08/privacy-lawsuit-over-gmail-will-move-forward/> accessed 25 October 2016

Naughton John, ‘Why the Internet of Things is the New Magic Ingredient for Cyber Criminals’ *The Guardian* (2 October 2016) <https://www.theguardian.com/commentisfree/2016/oct/02/brian-krebs-ddos-attack-google-protection-cybercrime>

Poe Robert, ‘The Ultimate Net Monitoring Tool’ *Wired* (17 May 2006) <http://www.wired.com/science/discoveries/news/2006/05/70914>

Rettman Andrew, ‘Security Fears Prompt US Scrutiny of EU Visa Waiver’ *Eu Observer* (23 February 2015) <https://euobserver.com/justice/127744>

Robinson Duncan and Foy Henry, ‘Poland Faces Brussels’ Ire over Media Reforms’ *Financial Times* (London, 14 January 2016)

Solon Olivia, ‘Yahoo Confirms 'state-sponsored' Hackers Stole Personal Data From 500m Accounts’ (23 September 2016) <https://www.theguardian.com/technology/2016/sep/22/yahoo-hack-data-state-sponsored>

Sprenger Polly, ‘Sun on Privacy: ‘Get Over It’’ *Wired* (26 January 1999) <http://archive.wired.com/politics/law/news/1999/01/17538>

Tonacci Fabio, ‘Terrorismo, la Rete Criptata: così la Cyber-jihad Comunica con i Lupi Solitari in Europa’ *La Repubblica* (26 July 2016) <http://www.repubblica.it/esteri/2016/07/26/news/terrorismo_rete_criptata_stato_islamico_cyber_jihad-144816976/>

Travis Alan, ‘Cybercrime Figures Prompt Police Call for Awareness Campaign’ *The Guardian* (21 July 2016) <https://www.theguardian.com/uk-news/2016/jul/21/crime-rate-online-offences-cybercrime-ons-figures> accessed 18 August 2016

Weiler Joseph HH, ‘¿Qué te Ha Pasado, Europa?’ *El País* (Madrid) 8 July 2016 <http://elpais.com/elpais/2016/07/06/opinion/1467803698_217589.html>

2.4 WEB SOURCES (BLOGS, WEBSITES, NEWSLETTERS)

Berners-Lee Tim, 'No Snooping' (<http://www.w3.org/DesignIssues/NoSnooping.html>, 2009)

European Digital Rights (EDRI), *US Agencies Have Unlimited Access to Internet Data* (EDRI-gram newsletter, n. 11.12 2013)

——, *What Digital Rights Are at Imminent Risk? All of Them* (EDRi-gram newsletter 14.17 2016)

European Network and Information Security Agency (ENISA), 'Glossary' (*ENISA*) <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary> accessed 2 February 2015

International Telecommunications Union (ITU), 'Global Cybersecurity Agenda (GCA)' <http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx> accessed 26 September 2016

Microsoft, 'SDL Threat Modeling Tool' (*Microsoft*) <https://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx> accessed 21 October 2016

——, 'Security Development Lifecycle' (*Microsoft*) <https://www.microsoft.com/en-us/sdl/> accessed 21 October 2015

——, 'Applying STRIDE' (*Microsoft*, 2005) <https://msdn.microsoft.com/en-us/library/ee798544%28v=cs.20%29.aspx> accessed 21 October 2016

——, 'The STRIDE Threat Model' (*Microsoft*, 2005) <https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx> accessed 21 October 2016

Muižnieks Nils, 'Human Rights at Risk When Secret Surveillance Spreads' (*The Council of Europe Commissioner's Human Rights Comment*, 24 October 2013) <https://www.coe.int/en/web/commissioner/-/human-rights-at-risk-when-secret-surveillance-sprea-1> accessed 16 August 2016

NetFort, *Unified Network Traffic Monitoring for Physical and VMWare Environments* (White Paper, 2010)

OSCE, Office for Democratic Institutions and Human Rights, 'ODIHR and the Rule of Law' <http://www.osce.org/odihr/103448>

OWASP, 'Application Threat Modelling' (*OWASP*) <https://www.owasp.org/index.php/Application_Threat_Modeling> accessed 21 October 2016

——, 'Threat Risk Modeling (wiki)' (*OWASP*) <https://www.owasp.org/index.php/Threat_Risk_Modeling> accessed 21 October 2016

Schneier Bruce, 'The Vulnerabilities Market and the Future of Security' (2013) <http://www.schneier.com/crypto-gram-1206.html> accessed 25 June

——, 'The NSA is Hoarding Vulnerabilities' (*CRYPTO-GRAM September 15*, 2016) <https://www.schneier.com/crypto-gram/archives/2016/0915.htm> accessed 15 September 2016

WikiLeaks, 'DotForce Newsletter - Giugno' (*Hacking Team*, 2015) <https://wikileaks.org/hackingteam/emails/emailid/92171>

2.5 SPEECHES AND LECTURES

Buttarelli Giovanni, 'Latest Developments in Data Protection' (Presentation at the meeting of the Heads of Agencies, Stockholm, 19 October 2012)

Corona Igino, 'Machine-Learning Approaches to the Detection of Fast Flux Networks and PDF malware' (Third Summer School on Security and Privacy: "Building Trust in the Information Age", Cagliari, September 2014)

Davies Bill, 'Bottom Up or Top Down - The History of Human Rights in European Law (speech)' (Setting An Agenda For Historical Research In European Law - Actors, Institutions, Policies and Member States, Florence, European University Institute, 11 December 2015)

Reding Viviane, *The Review of the EU Data Protection Framework, SPEECH/11/183* (2011)

—, *The EU's data protection rules and cyber security strategy: two sides of the same coin. Speech before the NATO Parliamentary Assembly/Luxembourg, SPEECH/13/436* (2013)

Rieck Konrad, 'Assisted Discovery of Vulnerabilities' (Third Summer School on Security and Privacy: "Building Trust in the Information Age", Cagliari, September 2014)

Zanero Stefano, 'Behavior-based Methods for Automated, Scalable Malware Analysis' (Third Summer School on Security and Privacy: "Building Trust in the Information Age", Cagliari, September 2014)

2.6 OTHER SOURCES

Eliot Thomas Stearns, 'Little Gidding' in Eliot Thomas Stearns (ed), *Four Quartets* (Harcourt 1943)