The Regulatory Effectiveness of Privacy by Design

Tomás Barbosa Pinto

Student Number	143726
Supervisor	Dr Nadezhda Purtova
Second Reader	Silvia De Conca LLM
Place and Date	Tilburg, 2017

Table of Contents

Introduction

Social problem and focus of the thesis

Privacy is a subjective notion that is shaped by time and the cultural and technological context.[1] In fact, it has been stated that "nobody can articulate what it means."[2] However, it is more and more difficult to ignore that without an adequate level of privacy, personal freedom is in jeopardy. This is supported by the notion that privacy is in the core of essential aspects of human rights such as personal freedom, autonomy and civil liberties.[3] In the same way, data protection or the right to data protection assumes equal relevance as one of the types of privacy.

Personal data is currently an important asset for society as the processing of person-related data is a practice transversal to individuals, governmental agencies and businesses. This is coupled by the alarmingly growing phenomenon of automatic processing of information and its storage in databases. The concern is that these bulks of such information are in part personal data.[4]

The technological developments that we witness result in various risks to those rights and are hand-in-hand with how data (including personal data) is now an asset in the digital economy. Due to these rapid technological developments that allow for the automatic processing of incredible sums of data from various interconnected sources, privacy and data protection has been object of the attention of both policy-making and academic literature.[5]

This reality represents an increase of risks of privacy and data protection rights violations that require the focus of regulation in order to balance the interests of the stakeholders.[6] In fact, the debate over the regulation of privacy and data protection is firmly connected with said technological developments as they pose a clear threat to one's privacy and data protection rights. These developments create several regulatory challenges as citizens and their representatives worry about the loss of control over personal data. At same time, it is also complicated to achieve the necessary regulatory balance of the threatened rights and

[1] Le Métayer D, 'Privacy by design: A matter of choice' [2010] Data Protection in a Profiled World 323–334.
[2] Solove DJ, Understanding privacy (Harvard University Press 2008).
[3] Badiul Islam M and Iannella R, 'Privacy by Design: Does It Matter for Social Networks?' in Jan Camenisch and others (eds), *Privacy and identity management for life: 7th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6 international Summer School, Trento, Italy, September 5-9, 2011, revised selected papers* (Springer-Verlag Berlin and Heidelberg GmbH & Co. K 2012) 207–220.
[4] Blarkom G. W., Borking J. J, and Olk J. G. E (eds), *Handbook of Privacy and Privacy-Enhancing Technologies - The case of Intelligent Software Agents* (ISBN 90 74087 33 7, College bescherming persoonsgegevens 2003).
[5] Koops B, 'The trouble with European data protection law' (2014) 4(4) International Data Privacy Law accessed 20 December 2015 250–261.
[6] Viola de Azevedo Cunha M, *Market integration through data protection: An analysis of the insurance and financial industries in the EU* (Springer 2013) page 3-4.

innovation. Consequently, the issue of regulating privacy and data protection is currently being considered as a top-priority in the political world.[7]

However, for the time being it seems as if the risks arising from technological developments are tackled in a way where technology is adapted to mitigate the problems after they come to light and when the damage is already done.[8] This is explained by the fact that those technologies – often referred to as Privacy Invading-Technologies (PITs) – are being developed and embraced at a pace that regulation cannot keep up with. Hence why they are often described as "disruptive". For these reasons, it has been claimed that recent technologies may have rendered global legal frameworks (and even the principles of privacy) inadequate.[9] This results in law and regulation being, as Klitou puts it, "behind the advancement of technology."[10]

Because of this situation it is necessary to consider privacy and protection in advance to overcome the insufficiencies of the current model. Thus, a change of paradigm is necessary. If the current manner through which the regulation of these issues is not adequate to the scenario described then it must be adapted. Being that the core problem is that the protection against those risks are mainly reactive in nature, then the approach has to be reversed.

Against this background, the Privacy by Design (PbD) approach is said to have the potential to solve the increasing problems of data subjects and their rights to privacy and data protection in the ever rising information society.[11] Namely, it prescribes an approach which intends to solve the problem mentioned above by taking Privacy and Data Protection early on (by design). For these reasons, the PbD approach has received considerable acceptance over the years by privacy regulators [12]and organisations.[13] In fact, this thesis is especially motivated by the inclusion of the approach in the recent EU General Data Protection Regulation[14](GDPR), which is a highly symbolic step to the adoption of this approach.

In this context, and given the lack of literature on matter, it is important to ascertain whether the adoption of Privacy by Design by EU regulators entails a sound and worthwhile regulatory intervention capable of enabling the pursuit of Privacy and Data Protection goals. The approach has been discussed in the legal scholarship as to its merits and how its principles should be interpreted and applied[15]. From the computer science side, there is a claim for a more explained guidance on the application of the principle at

[7]Busch A, 'The regulation of privacy' in Levi-Faur David (ed), Handbook on the Politics of Regulation (Edward Elgar Publishing 2011).
[8] Krebs D, ''Privacy by Design': Nice-to-Have or a Necessary Principle of Data Protection Law?' (2013) Vol. 4, 2013 JIPITEC.
[9] Klitou D, 'Privacy by design and privacy-invading technologies: Safeguarding privacy, liberty and security in the 21st century' (2011) 5(3) Legisprudence 297–329, page 298.
[10] Klitou D, 'Privacy by design and privacy-invading technologies: Safeguarding privacy, liberty and security in the 21st century' (2011) 5(3) Legisprudence 297–329, page 297.
[11] Information and Privacy Commissioner/Ontario, Landmark Resolution passed to preserve the Future of Privacy, http://www.ipc.on.ca/images/Resources/2010-10-29-Resolution-e_1.pdf
[12] Rubinstein, Ira, Regulating Privacy by Design (May 10, 2011). Berkeley Technology Law Journal, Vol. 26, p. 1409, 2012. Available at SSRN: http://ssrn.com/abstract=1837862 .
[13] Information and Privacy Commissioner/Ontario, Landmark Resolution passed to preserve the Future of Privacy, http://www.ipc.on.ca/images/Resources/2010-10-29-Resolution-e_1.pdf
[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[15] Koops B-J and Leenes R, 'Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law' (2013) 28(2) International Review of Law, Computers & Technology 159–171. DOI:10.1080/13600869.2013.801589

the design level.[16] Even though there is literature on the criticism and commendations of the PbD approach, they do not conclude with the regulatory effectiveness of its adoption in EU Law. In fact, it has been stated that there is still no adequate method to evaluate the effectiveness of laws and mechanisms in protecting privacy.[17] While that might not be the case, the fact is that there is a gap in literature lacking of discussion of testing the effective normative regulatory design of PbD. There are methods to compare the outputs and outcomes of regulatory interventions.[18] However, since the legislation – the most important input by the legislator on the adoption of the PbD approach – is not yet in force, such method cannot be leveraged just yet. Thus, by performing an a priori effectiveness assessment focusing on regulatory design, this thesis will fill a hole in the literature.

In order to do so, not only is it relevant to analyse the legislation that explicitly incorporated the approach, but also to consider its broader regulatory design. Thus, this thesis aims to establish whether this adoption of the approach in EU Law, promoting Privacy by Design, meets the requirements of effective regulatory design.

The object of the thesis is the incorporation of the Privacy by Design regulatory approach in EU Law, where the legislator took the approach of adopting the term in legislation as "Data Protection by Design and by Default". Regardless, this thesis will focus on both the concepts of Privacy and Data Protection as PbD is an approach that accommodates for both. Furthermore, regulators in general and the discussion at hand in particular do not benefit from limiting the scope in such a way. Thus, we will refer to PbD throughout the text, sometimes as a regulatory approach to privacy and data protection, while discussing its adoption on EU Law.

Privacy by Design

Privacy by Design is the approach focused on maximizing privacy and data protection by embedding safeguards across the design and development of products, services or processes by taking privacy and data protection considerations into account from the outset and throughout their whole lifecycle, rather than as a remedial afterthought. Said safeguards should be built into the core of the products, services or processes and treated as a default setting for not only technologies, but also "operation systems, work processes, management structures, physical spaces and networked infrastructures"[19]. For the purpose of this thesis, it is important as well to understand it as a regulatory approach that can be adopted in policy whereby its adoption comprises of a regulatory intervention (such as the EU case). The latter is the main object of this thesis.

The Privacy by Design approach traces back to the emergence of Privacy-Enhancing Technologies (PETs) in the 1990's as an alternative for the conventional use of legal and administrative tools through which there is merely a policy-making and monitoring process towards enforcement. PETs originated from

[16] See Wiese Schartum D, 'Making privacy by design operative' (2016) 24(2) International Journal of Law and Information Technology 151–175.
[17] Bennet, C and Raab, C, 'The Governance of Privacy: Privacy Instruments in global perspective' (2003), page 196.
[18] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008).
[19] Davies S, 'Why privacy by design is the next crucial step for privacy protection' [2010], http://i-comp.org/wp-content/uploads/2013/07/privacy-by-design.pdf accessed 14 October 2016

concepts of "data protection by technology"[20] and "Privacy by Design"[21] and gained reputation through them.[22] However, in recent times Privacy by Design has progressively replaced the concept of PETs and even though it is a concept recurrently used as a synonym for PETs, it is more accurately described as the idea behind it.[23]

According to its original developer, Ann Cavoukian, Privacy by Design is an approach to privacy which cannot be accomplished merely by privacy and data protection laws, but rather by privacy becoming a default mode for organisations. Her "7 Foundational Principles"[24] require that data protection should be a fundamental component of every system, technology, service or product and should be taken into account throughout their development, use and disposal, by all the actors involved in a transparent manner. She believes that using such a proactive and preventive approach benefits all the stakeholders involved, ensuring protection of the data subject's fundamental rights.[25]

Privacy by Design is transversal to IT systems, business practices (organisations) and physical design.[26] In fact, Privacy by Design is a product of different disciplines such as law and computer science and it follows that it was envisioned as something to be set up as a practice in organisations, codified in laws (pieces of legislation) and as way to enforce law by itself. Accordingly, Tsormpatzoudi et al. have highlighted that even though the concept of PbD is yet to be properly disseminated through the general public and the industry, there is an opportunity to merge "research and policy together"[27].

For its advocates, Privacy by Design (PbD) represents the paradigmatic change from the traditional and outdated approaches to privacy and data protection which solely focus on setting minimum requirements for information management practices, and relying on remedies for privacy breaches in a post factum, manner[28]. The former Berlin Commissioner for Data Protection and Freedom of Information described soundly these practices as "locking the stable door after the horse has bolted"[29] and identifies this approach as the one used by other fellow Data Protection Commissioners and other regulators.[30] Cavoukian

[20] ULD (1996). Sommerakademie Datenschutz durch Technik – Technik im Dienste der Grundrechte. [Summer Academy Data Protection by Technology – Technology at the Service of Fundamental Rights.] https://www.datenschutzzentrum.de/sommerakademie/1996/sa96prog.htm; Summarised in a report available at https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/52DSK-KurzberichtZumDatenschutzDurchTechnik.pdf?blob=publicationFile

[21] Cavoukian A, '7 Foundational principles' (August 2009) <https://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/> accessed 2 November 2015.

[22] Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers (Springer 2016) 199–212.

[23] Koops B-J and Leenes R, 'Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law' (2013) 28(2) International Review of Law, Computers & Technology 159–171. DOI:10.1080/13600869.2013.801589

[24] Cavoukian A, '7 Foundational principles' (August 2009) <https://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/> accessed 2 November 2015.

[25] Cavoukian A, '7 Foundational principles' (August 2009) <https://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/> accessed 2 November 2015.

[26] Kindt E, *Privacy And Data Protection Issues Of Biometric Applications* (Springer Netherlands 2013).

[27] Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers (Springer 2016) 199–212.

[28] Cavoukian A and Harbour P, 'Foreword By: Privacy By Design In Law, Policy And Practice' (2011) https://www.ipc.on.ca/images/resources/pbd-law-policy.pdf accessed 29 February 2016

[29] Dix A, 'Built-In Privacy—No Panacea, But A Necessary Condition For Effective Privacy Protection' (2010) 3 Identity in the Information Society, page 257.

[30] Dix A, 'Built-In Privacy—No Panacea, But A Necessary Condition For Effective Privacy Protection' (2010) 3 Identity in the Information Society.

further stated that its aims are ensuring privacy and ensuring control over personal information in one hand, and in the other hand, for organizations to obtain a competitive advantage.[31]

Regulatory effectiveness

Even though it is necessary to be cautious when dealing with the concept of regulation, being that is troublesome to define precisely[32],[33] the definition of regulation used in this thesis is the one by Black who understands regulation as 'the intentional use of authority to affect behaviour of a different party according to set standards, involving instruments of information-gathering and behaviour modification'.[34]

As far as regulatory effectiveness is concerned, to begin with and for the purpose of this thesis, it is sufficient to define regulatory effectiveness merely as how well a regulatory intervention is designed in order to meet its stated purposes. When it comes to effectiveness, generally, regulators cannot be judged as to whether they are doing the "right thing"[35], but rather as to whether they are doing it in "the right kind of way"[36]. According to Brownsword, in order to regulate in the right kind of way or to regulate effectively, regulators have to be clear about their goals, smart in the approach and regulate along the values of the regulatees.[37] Hence, for the purpose of this thesis it is relevant to ascertain whether the regulatory intervention of adopting PbD in EU Law fulfils these effective regulatory design criteria.

Methodology and argument roadmap

The approach to the questions at hand was based on the analysis of theories of regulation and theories that inform effective regulatory design, determining the most adequate criteria for the assessment at hand and analyse them against the relevant aspects of the incorporation of PbD by the EU regulator.

The first chapter will serve to describe the PbD approach. Namely, explaining the concept of PbD, analysing how it became an internationally recognized approach to Privacy and Data Protection and analysing the incorporation of the approach in EU Law (GDPR and the ePrivacy Regulation). Thus, this chapter is purposed to answer the sub-question "What is PbD?"

The second chapter provides an overview of the selected criteria found in the literature that informs the effective regulatory design assessment of this thesis, the way the concept of regulation is perceived nowadays. There, the Proposed Framework for evaluation is presented. This chapter will generally answer the sub-question: "What makes for effective regulatory design?"

---

[31] Cavoukian A, '7 Foundational principles' (August 2009) <https://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/> accessed 2 November 2015.
[32] Morgan B and Yeung K, *An introduction to law and regulation: Text and materials* (Cambridge University Press 2007).
[33] Baldwin R, Cave M, and Lodge M, *Understanding regulation: Theory, strategy, and practice* (2nd edn, Oxford University Press 2012).
[34] Baldwin, R., Cave, M. and Lodge, M. (2010). Introduction: Regulation—the Field and the Developing Agenda. *Oxford Handbooks Online*, page 6.
[35] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008).
[36] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008).
[37] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008).

Finally, the third chapter will bring the previous two together in the sense that the takeaways from each of them will be crossed in order to determine the degree of effectiveness of the European PbD regulatory intervention. This chapter will lay the reasoning that ultimately leads to the Conclusion where the ultimate answer of this thesis is advanced: Does the PbD incorporation in EU Law observe criteria of effective regulatory design?

Chapter 1: Privacy by Design

1.1 Introduction

The right to data protection and the individual right to privacy are being threatened by the technological turbulence and the contexts of the informational age. Thus, the debate surrounding these threats is taking place led by academics and regulators. To address this, and to shift the traditional ways in how these threats have been dealt with and how to preserve the above mentioned rights, the approach of PbD has been proposed. Increased relevance is brought to this approach with its inclusion in the recent General Data Protection Regulation[38]. In this chapter, we will explore this vision pointing out its characteristics and developments. Thus, this first chapter is dedicated to the analysis of Privacy by Design. Firstly, the concept or its definition is explored in section 1.2. In section 1.3 its origins are laid out to better understand the context and the development of the notions that surround it. Section 1.4 is dedicated to the incorporation of the approach in EU Law. Section 1.5 rounds up with a conclusion. By doing so, and by highlighting its aspects and characteristics, ultimately it will be possible to combine them with the criteria for regulatory effectiveness and answer the main question of this thesis.

1.2 The Concept

Privacy by Design is the approach focused on maximizing privacy and data protection by embedding safeguards across the design and development of products, services or processes by taking privacy and data protection considerations into account from the outset and throughout their whole lifecycle, rather than as a remedial afterthought.[39] Said safeguards should be built into the core of the products, services or processes and treated as a default setting for not only technologies, but also "operation systems, work processes, management structures, physical spaces and networked infrastructures"[40].

The concept of PbD had the contribution of many privacy experts and gathered a respectable number of advocates that further helped the dissemination and development of the concept.[41] However, in its core the concept draws much from Cavoukian's '7 Foundational Principles'[42] that in turn were inspired

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

[39] Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers(Springer 2016) 199–212; Koops B-J and Leenes R, 'Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law' (2013) 28(2) International Review of Law, Computers & Technology 159–171. DOI:10.1080/13600869.2013.801589; Davies S, 'Why privacy by design is the next crucial step for privacy protection' [2010], http://i-comp.org/wp-content/uploads/2013/07/privacy-by-design.pdf accessed 14 October 2016, page 2.

[41] Krebs D, ''Privacy by Design': Nice-to-Have or a Necessary Principle of Data Protection Law?' (2013) Vol. 4, 2013 JIPITEC.

[42] Cavoukian A, '7 Foundational principles' (August 2009), <https://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/> accessed 2 November 2015

by Fair Information Practices (FIPs)[43]. Cavoukian's principles remain the core of the notion of PbD.[44] For example, they are one of the starting points for software developers that want to take privacy and data protection into account when designing information systems.[45] The sum of these principles embodies the goals of PbD: "ensuring privacy, gaining control over one's information, and, for organizations, gaining a 'sustainable competitive advantage.'"[46]

The '7 foundational principles'[47] are:

1) "*Proactive not Reactive; Preventative not Remedial*" - this principle requires that privacy and data protection are approached in proactive rather than reactive terms. This makes PbD preventive and not merely remedial.[48] In this way, privacy risks are anticipated and prevented before they materialize.[49]

2) "*Privacy as the Default*"; - the idea is that privacy and data protection are automatically safeguarded in every system as its default position.[50] Thus, PbD aims at providing the maximum level of privacy and data protection "by ensuring that personal data are automatically protected in any IT system or business practice"[51]. This way there is no need for the individual to take action to protect their privacy - as it is automatically protected, designed into the system by default.[52]

3) "*Privacy Embedded into Design*"; - accordingly the protection is in the core of systems and business practices rather than a remedial patch which ensures that privacy and data protection are a fundamental feature of a given functionality of a system.

4) "*Full functionality: Positive-sum not zero-sum*"; - in order to gather all the interests and objectives, PbD negates avoidable trade-offs such as privacy vs. security.

5) "*End-to-end Lifecycle Protection*;" - this means that PbD applies throughout the whole lifecycle of the processing. Before the first data are collected, PbD is already in place and it is extended to the end of the cycle, f.e ensuring also that at the end of the processing data are erased timely.

6) "*Visibility and transparency*"; - this requires accountability from whatever business practice or technology involved in order to reassure every stakeholder that in fact PbD criteria are being practiced by maintaining all operations visible and transparent.

7) "*Respect for user privacy*;" - this places the respect for the user's interest as a prominent criteria of the whole process making PbD individual-focused.

---

[43] FIPs or FIPPs (Fair Information Practice Principles) are universal privacy principles for handling personal data. They serve as guidelines that represent widely accepted concepts concerning fair information practice; Cavoukian A, 'Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers' [2011] <https://privacybydesign.ca/content/uploads/2011/08/pbd-law-policy.pdf> accessed 12 November 2015.

[44] Krebs D, "Privacy by Design': Nice-to-Have or a Necessary Principle of Data Protection Law?' (2013) Vol. 4, 2013 JIPITEC.

[45] Wiese Schartum D, 'Making privacy by design operative' (2016) 24(2) International Journal of Law and Information Technology 151–175.

[46] Cavoukian A, '7 Foundational principles' (August 2009),<https://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/> accessed 2 November 2015; Krebs D, "Privacy by Design': Nice-to-Have or a Necessary Principle of Data Protection Law?' (2013) Vol. 4, 2013 JIPITEC.

[47] Cavoukian A, '7 Foundational principles' (August 2009).

[48] Pagallo U, 'On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law' in Serge Gutwirth and others (eds), *European data protection: In good health?* (Springer Science & Business Media 2012) 342.

[49] Cavoukian A, '7 Foundational principles' (August 2009).

[50] Pagallo U, 'On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law' in Serge Gutwirth and others (eds), *European data protection: In good health?* (Springer Science & Business Media 2012) 342.

[51] Cavoukian A, '7 Foundational principles' (August 2009) page 2.

[52] Cavoukian A, '7 Foundational principles' (August 2009).

It is important to stress that PbD was developed and influenced by law and computer science as it was purposed as something to be codified into legal instruments, as a way to enforce such laws through technology and to be put in practice in organisations. From a regulatory point of view, PbD is an approach to privacy protection that uses technology to advantage of the law in the sense that it aids enforcing legal provisions. This use of technology as a regulatory instrument has been described as "code as law"[53] by Lessig[54]; Brownsword[55] termed it as "techno-regulation"[56]. The approach seeks to identify and minimize privacy risks and resorts to technical solutions to enforce the legal requirements of privacy and data protection.[57] From the policy and legal realm, contributions arose from the debate and reflections on the merits and limitations of this approach as a solution for privacy and data protection enforcement.[58]

On the technological side, the contribution was the production of privacy-respecting tools or design methods. The use of the PbD approach in computer science is developing and can be identified in tools or instruments such as Privacy-Enhancing Technologies (PETs), design guidelines, processes and practices.[59] The means range from mathematical proofs[60] of datasets and algorithms (tweaked to have certain qualities or by placing constraints on them) to research of privacy related human behaviour, of how to construct human-computer interfaces and maturing methodologies for requirements engineering and software development. Since the moment the concept was first developed, its focus shifted from identity shielding to more generally prescribing the design of systems where privacy and data protection rules are automatically enforced as much as possible and the collection of data, storage and sharing are reduced to the minimum required to achieve the functionality for which the system is designed for.

Currently, however, it is a truly multifaceted concept that involves different technological and organizational aspects that aim for the implementation of privacy and data protection principles. The concept draws from both the legal perspective that define it as a more general principle and from the engineers and computer scientists that rather relate it with the development and deployment of Privacy-Enhancing Technologies (PET's – which we will discuss in section 2.3).[61]

---

[53] Koops B.-J, Bodea G, Hoepman J-H, Leenes R, Vedder A, D3.4 Code as Code Assessment (VIRTUOSO FP7 project (2009); Lessig L, *Code: And other laws of Cyberspace* (3rd edn, Basic Books 1999).
[54] Lessig L, *Code: And other laws of Cyberspace* (3rd edn, Basic Books 1999).
[55] Brownsword, R. (2004), 'What the World Needs Now: Techno-Regulation, Human Rights and Human Dignity'. in: Global Governance and the Quest for Justice (edited by Brownsword, R.). 4: Human Rights. Hart, p. 203-234.
[56] Brownsword, R. (2004), 'What the World Needs Now: Techno-Regulation, Human Rights and Human Dignity'. in: Global Governance and the Quest for Justice (edited by Brownsword, R.). 4: Human Rights. Hart, p. 203-234.
[57] Tsormpatzoudi P, Coudert F, PRIPARE, Deliverable D5.1 State-of-Play: Current Practices and Solutions (2014) http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE_Deliverable_D5.1_v1.0.pdf
[58] Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers(Springer 2016) 199–212;
[59]Gurses S, Troncoso C and Diaz C, 'Engineering Privacy By Design', *Conference on Computers, Privacy and Data Protection (CPDP 2011)* (2011) https://lirias.kuleuven.be/bitstream/123456789/356725/1/article-1542.pdf accessed 20 September 2016; Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers(Springer 2016) 199–212.
[60] A mathematical proof is a deductive argument for a mathematical statement. A proof can be traced back to self-evident or assumed statements, known as axioms, along with accepted rules of inference (Wikipedia).
[61] ENISA, 'Privacy by design in big data - information technology and telecommunications - EU Bookshop' [2015] <http://dx.doi.org/10.2824/641480> accessed 15 October 2016.

While elaborating on the concept of PbD, both in the literature and in the GDPR (see Section 1.4), it is possible to single out an accessory principle to Privacy by Design that is Privacy by Default.[62] As mentioned, the concept of Privacy by Default is also one of the "Foundational Principles" of Cavoukian's influential conception of Privacy by Design. Marit Hansen perceives Privacy by Default as being double-faced[63]. On the one hand, it means that the principle requires that Privacy by Design should be "business as usual" (as Hansen puts it – a "matter of course"), in the sense that taking the PbD approach should be the customary and natural manner in which ICT systems are designed and operated. On the other hand, its other meaning is that when designing the ICT systems, the configuration of the default settings is made with privacy-friendly standards in such a way that, by default, privacy and data protection are as most safeguarded as possible.[64] In other words, privacy-friendly standards in a given system's settings are always "turned on" by default. This renders enforcement interventions redundant and mitigates risks that f.e result from user's lack of knowledge about the impact of their choices and privacy and data protection considerations.[65]

As a concluding remark on the concept of PbD, it is important to point out that the approach is purposed as something to be codified into legal instruments, as a way to enforce such laws through technology and to be put in practice in organisations. In fact, the concept of PbD can be explained as what the principle entails, that is, in simple terms, that privacy and data protection safeguards should be embedded in whatever relevant proposition (product, process, service, system, etc.) in the early stages of development as a default. That is the core meaning of PbD and something to be adopted by every stakeholder when dealing with such propositions and applying the principle. But also, on a more high-level, as an approach to tackle privacy and data protection from a regulatory point of view. Adopting a regulation pursuant to PbD entails recognizing and facilitating the use of technology as a regulatory instrument to pursue Privacy and Data Protection goals, and prescribing the adoption of Privacy by Design *modus operandi* (Cavoukian's 7 principles). Thus, PbD must be understood as having two dimensions: one relates to adopting the approach in the context of data processing activities and development of products, services technologies; the other relates to the regulatory approach to Privacy and Data Protection. These two meanings or points of view are in a constant interplay throughout the text of this thesis. However, it shall be considered that when referring to a producer, organisation or controller adopting the PbD approach, then it shall mean, roughly, that they follow Cavoukian's 7 foundational principles or whatever interpretation of what the principle entails by a given legislator/regulator. When referring to the regulator, or legislator's choices in regulating the subject, then it shall mean that they followed the approach on a regulatory process level.

[62] Tsormpatzoudi P, Coudert F, PRIPARE, Deliverable D5.1 State-of-Play: Current Practices and Solutions (2014).
[63] Hansen M, "Data Protection by Default in Identity-Related Applications" in Simone Fischer-Hübner, Elisabeth de Leeuw, and Chris Mitchell (eds), *Policies and Research in Identity Management: Third IFIP WG 11.6 Working Conference, IDMAN 2013* (2013).
[64] Hansen M, "Data Protection by Default in Identity-Related Applications" in Simone Fischer-Hübner, Elisabeth de Leeuw, and Chris Mitchell (eds), *Policies and Research in Identity Management: Third IFIP WG 11.6 Working Conference, IDMAN 2013* (2013).
[65] Tsormpatzoudi P, Coudert F, PRIPARE, Deliverable D5.1 State-of-Play: Current Practices and Solutions (2014). http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE_Deliverable_D5.1_v1.0.pdf

1.3 Origins, Development and Context

The origins of the concept takes us as far as the 1960s, and to the architecture and building sectors where privacy was a weighed factor in the construction of residential buildings and site developments.[66] But it only emerged in the context of the information society as of the mid-1990s[67] based on pre-existing concepts such as "code as law"[68] and "value-sensitive design".[69] Curiously it appeared after the term "Surveillance by Design" was created, which resulted from the debate over an US legislation that intended to ensure that communication systems were designed to ensure surveillance capabilities in order to allow law enforcement to access whatever data they wanted (by embedding such capabilities into the communication systems). S. Davies believes that in some ways PbD was a correspondent response to it.[70]

The origins of the term with respect to the context at hand was first discussed in "Privacy Enhancing Technologies: the path to anonymity"[71], a report that resulted from the collaboration of the Dutch Data Protection Authority and the Information and Privacy Commissioner for the Province of Ontario, Canada.[72] It was then that, together with the concept of Privacy-Enhancing Technologies, the approach first emerged.[73] As a matter of fact, Ann Cavoukian, the former Privacy Commissioner of Ontario - regarded as the creator of Privacy by Design, departed from the concept of PETs to develop the PbD approach and it has done so extensively.[74] The appearance of these concepts aimed at providing an alternative to the common legal and administrative efforts that solely consisted of policy-making and compliance monitoring.[75] The mentioned report was one of the first times that privacy was approached or discussed from a designer's perspective.[76] Then, the term "Privacy by Design" was expressly mentioned in a workshop that took place in the "Computers, Freedom & Privacy 2000: Workshop on Freedom and Privacy

[66] Davies S, 'Why privacy by design is the next crucial step for privacy protection' [2010], http://i-comp.org/wp-content/uploads/2013/07/privacy-by-design.pdf accessed 14 October 2016.
[67] Davies S, 'Why privacy by design is the next crucial step for privacy protection' [2010], <http://i-comp.org/wp-content/uploads/2013/07/privacy-by-design.pdf> accessed 14 October 2016.
[68] Lessig L, *Code: And other laws of Cyberspace* (3rd edn, Basic Books 1999).
[69] Koops B-J and Leenes R, 'Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law' (2013) 28(2) International Review of Law, Computers & Technology 159–171. DOI:10.1080/13600869.2013.801589.
[70] Davies S, 'Why privacy by design is the next crucial step for privacy protection' [2010], http://i-comp.org/wp-content/uploads/2013/07/privacy-by-design.pdf accessed 14 October 2016.
[71] Hes, R., Borking, J.: Privacy Enhancing Technologies: the path to anonymity (Revised Edition) Registratiekamer, Achtergrondstudies en Verkenningen 11 (first edition 1995); van Rest J and others, 'Designing Privacy-by-Design' in B Preneel and D Ikonomou (eds), Privacy Technologies and Policy - First Annual Privacy Forum, APF 2012 Limassol, Cyprus, October 2012 Revised Selected Papers(2014).
[72] Easton C, 'Information Systems for Crisis Response and Management: The EU Data Protection Regulation, Privacy by Design and Certification' (Short Paper – Ethical, Legal and Social Issues Proceedings of the ISCRAM 2016 Conference – Rio de Janeiro, Brazil, May 2016 Tapia, Antunes, Bañuls, Moore and Porto de Albuquerque, eds.); Hustinx P, 'Privacy by design: Delivering the promises' (2010) 3(2) Identity in the Information Society http://dx.doi.org/10.1007/s12394-010-0061-z accessed 25 February 2016 253–255
[73] Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers(Springer 2016) 199–212.
[74] Tsormpatzoudi P, Coudert F, PRIPARE, Deliverable D5.1 State-of-Play: Current Practices and Solutions (2014).
[75] Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers(Springer 2016) 199–212.
[76] Hes, R., Borking, J.: Privacy Enhancing Technologies: the path to anonymity (Revised Edition) Registratiekamer, Achtergrondstudies en Verkenningen 11 (first edition 1995); van Rest J and others, 'Designing Privacy-by-Design' in B Preneel and D Ikonomou (eds), Privacy Technologies and Policy - First Annual Privacy Forum, APF 2012 Limassol, Cyprus, October 2012 Revised Selected Papers(2014).

by Design" conference. In the meantime, the PISA project, which focused on Privacy Incorporated Software Agents, also worked with the terms PbD and PETs.[77]

Since then, the approach achieved some traction and both PETs and PbD gathered reputation and recognition.[78] Concerning the EU, in 2007, the European Commission issued a Communication "on Promoting Data Protection by Privacy Enhancing Technologies"[79] that promoted data protection by PETs as a complementary mechanism for the enforcement of the data protection framework and delineated three objectives: to support the development of PETs, support their use by data controllers and also by the consumers. In 2009, in the context of the reform of EU data protection framework, some of reflection on the matter of PbD was brought up by the Article 29 Working Party, together with the Working Party on Police and Justice. In their Joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data[80] the incorporation of a principle of PbD is promoted. The implementation of PETs is also advocated for and deemed to be necessary given the importance of PbD, together with the implementation of "privacy by default"/default settings and personal data protecting tools such as encryption and access control.[81] In the same way, in 2010, the EDPS recognized that the manner in which the data protection framework was worded at the time did not provide with sufficient clarity for a requirement of PbD in the design of systems. Thus, similarly to the Article 29 Working Party, the EDPS[82] stressed the need to incorporate PbD in the data protection framework by recommending it as a general principle and that it should be contained in the provisions of specific legal instruments; moreover, it defended the incorporation of the principle in the Digital Agenda for Europe and also another technological related EU initiatives.[83] Another Communication in 2010 further promoted PETs together with PbD and stressed the importance of the deployment of these technologies in order to "ensure that data controllers put in place effective policies and mechanisms to ensure compliance with data protection rules".[84]

The international recognition of the principle was marked by the Privacy by Design Resolution[85] proposed by Cavoukian and endorsed by other Information and Privacy Commissioners. It was resolved to "recognize PbD as essential component of fundamental privacy protection; encourage the adoption of PbD's Foundational Principles (...) as guidance to establishing privacy as an organization's default mode of operation; and invite Data Protection and Privacy Commissioners/Authorities to promote PbD, foster its

[77] van Rest J and others, 'Designing Privacy-by-Design' in B Preneel and D Ikonomou (eds), *Privacy Technologies and Policy - First Annual Privacy Forum, APF 2012 Limassol, Cyprus, October 2012 Revised Selected Papers*(2014).
[78] Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers(Springer 2016) 199–212.
[79] European Commission, *Communication from the commission to the European parliament and the council on promoting data protection by privacy enhancing technologies (PETs)* COM/2007/0228 final (2007).
[80] Working Party (WP) Article 29 D-95/46/EC.2009. The Future of Privacy. 02356/09/EN-WP 168.
[81] Working Party (WP) Article 29 D-95/46/EC.2009. The Future of Privacy. 02356/09/EN-WP 168.
[82] EDPS, Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, OJ C 280/01 (2010).
[83] Tsormpatzoudi P, Coudert F, PRIPARE, Deliverable D5.1 State-of-Play: Current Practices and Solutions (2014).
[84] European Commission, *Communication from the commission to the European parliament, the council, the economic and social committee and the committee of the regions: a comprehensive approach on personal data protection in the European union* COM(2010) 609 final (2010).
[85] Privacy by Design Resolution at the 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem, 27 - 29 October 2010. Available online at http://www.privacyconference2011.org/htmls/adoptedResolutions/2010_Jerusalem/2010_J5.pdf

incorporation and encourage its research"[86]. In the United States, the momentum behind the principle has been also noteworthy. Between 2009 and 2010 the U.S Federal Trade Commission (FTC) organized several public discussions on privacy that resulted in the Center for Democracy and Technology recommending that the FTC would incentivize the adoption of business practices consistent with the PbD principle.[87] Consequently, the FTC issued a staff report [88] describing a Proposed Framework with three main components, being one of them PbD.[89]

As the origins of PbD are so connected with PETs in this section we will analyse it with some more depth. The introduction and development of Privacy Enhancing Technologies was crucial to the development of PbD.[90] In fact, they are closely connected. PETs were first introduced in the report "Privacy-enhancing technologies: the path to anonymity"[91], published in 1995. The report introduced the new vision to privacy protection by showcasing a number of cases that support the argument that systems can have equal functionalities while processing a considerable smaller amount of personal data, or no personal data at all.[92] Despite the different definitions, PETs can be described as "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system".[93]

Since the report, the vision of embedding privacy and data protection in the design of systems has been debated. Prior work on confidentiality, or anonymity and pseudonymity proved that technology could contain privacy and data protection safeguards and considerations.[94] In fact, PETs were originally developed to address data quality and data security (aimed at ensuring confidentiality of personal data), but gradually also became a solution for other data principles such as transparency or accountability[95] and more importantly for the principle of data minimization, which is intrinsically related with the concept of PETs. Therefore, in general PETs grew as a solution for personal data management and data minimization.

---

[86] Privacy by Design Resolution at the 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem, 27 - 29 October 2010. Available online at http://www.privacyconference2011.org/htmls/adoptedResolutions/2010_Jerusalem/2010_J5.pdf

[87] Cavoukian A, 'Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers' [2011] <https://privacybydesign.ca/content/uploads/2011/08/pbd-law-policy.pdf> accessed 12 November 2015.

[88] BUREAU OF CONSUMER PROTECTION, FED. TRADE COMM'N (FTC), PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2010).

[89] Rubinstein I, 'Regulating Privacy by Design' (2011) Vol.26 Berkeley Technology Law Journal (2012) 1409–1456.

[90] Tsormpatzoudi P, Coudert F, PRIPARE, Deliverable D5.1 State-of-Play: Current Practices and Solutions (2014) http://prip areproject.eu/wp-content/uploads/2013/11/PRIPARE_Deliverable_D5.1_v1.0.pdf

[91] Information and Privacy Commissioner/Ontario, *Privacy-enhancing technologies: The path to anonymity* (John J. Borking and Ronald Hes eds, Registratiekamer 1995).

[92] Hustinx P, 'Privacy by design: Delivering the promises' (2010) 3(2) Identity in the Information Society http://dx.doi.org/10.1007/s12394-010-0061-z accessed 25 February 2016 253–255

[93] EU-funded PISA project's definition; European Commission, *Communication from the commission to the European parliament and the council on promoting data protection by privacy enhancing technologies (PETs)* COM/2007/0228 final (2007).

[94] Hoepman J-H, Hansen M, and Jensen M, 'Towards measuring maturity of privacy-enhancing technologies' in Bettina Berendt and others (eds), *Privacy Technologies and Policy - Third Annual Privacy Forum, APF 2015 Luxembourg, Luxembourg, October 7–8, 2015 Revised Selected Papers* (Springer Science + Business Media 2016) 3–20.

[95] Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers(Springer 2016) 199–212.

Ultimately, they developed into the concept of PbD as a more overarching concept, applicable in scope not only to ICT systems, but for organisations, methods and practices as well.[96]

Even though they partially overlap and they have been used interchangeably, currently the two concepts are not the same. PETs are applications that focus on an unique component of privacy such as anonymity, confidentiality and control of information, usually deployed into pre-existing systems. In some occasions they are used as an afterthought by designers and by end-users with some privacy awareness. In turn, PbD is rather a "systematic approach" towards the design of any technology or product where privacy is embedded to the object's architecture".[97] In other words, whereas PETs aimed at exploring the positive side of technology by bolting privacy controls into systems, PbD dictates that privacy requirements are automatically inserted in the design and operation of not only a product or technology, but to all data processing environments.[98] Basically, Privacy by Design is the "idea behind PETs".[99] PETs are one of the measures or tools that may be employed to meet aims of Privacy by Design. Privacy threats can be tackled by developing new PETs or relying on existing ones in order to fulfil PbD requirements.[100]

The adoption of such technologies was considerable over the last decades and the concept experienced an embrace from policy and research. The European Union was one of the important sponsors of PETs.[101] Such support is patent in the Commission's Communications of 2007[102] and 2010[103] already mentioned above.

1.4 How PbD has been adopted in EU Policy

Even though there was no previous explicit inclusion of the principle of PbD in legislations, the idea of incorporating technological data protection safeguards is not entirely new. In fact, where it comes to EU Law, the Directive 95/46/EC[104] contains provisions with the same rationale. Such is the case of article 17 where it is provisioned that data controllers shall implement "*appropriate technical and organizational measures*"[105]; and also in the recital 46 that demands that those measures are taken "*both at the time of the*

[96]Hustinx P, 'Privacy by design: Delivering the promises' (2010) 3(2) Identity in the Information Society http://dx.doi.org/10.1007/s12394-010-0061-z accessed 25 February 2016 253–255.
[97] Rubinstein I, 'Regulating Privacy by Design' (2011) Vol.26 Berkeley Technology Law Journal (2012) 1409–1456.
[98] Davies S, 'Why privacy by design is the next crucial step for privacy protection' [2010], http://i-comp.org/wp-content/uploads/2013/07/privacy-by-design.pdf accessed 14 October 2016.
[99] Koops B-J and Leenes R, 'Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law' (2013) 28(2) International Review of Law, Computers & Technology 159–171. DOI:10.1080/13600869.2013.801589
[100] Rubinstein I, 'Regulating Privacy by Design' (2011) Vol.26 Berkeley Technology Law Journal (2012) 1409–1456.
[101] Koops B-J and Leenes R, 'Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law' (2013) 28(2) International Review of Law, Computers & Technology 159–171. DOI:10.1080/13600869.2013.801589
[102] European Commission, *Communication from the commission to the European parliament and the council on promoting data protection by privacy enhancing technologies (PETs)* COM/2007/0228 final (2007).
[103] European Commission, *Communication from the commission to the European parliament, the council, the economic and social committee and the committee of the regions: a comprehensive approach on personal data protection in the European union* COM(2010) 609 final (2010).
[104] Directive 95/46/EC (Directive on protection of individuals with regard to the processing of personal data and on the free movement of such data).
[105] Directive 95/46/EC (Directive on protection of individuals with regard to the processing of personal data and on the free movement of such data).

design of the processing system and at the time of the processing itself"[106]. Besides those, article 16 of the same directive and article 14/3 of the ePrivacy Directive[107] contain identical provisions that mirror the ones that, as we will see, were included explicitly for the first time in legislation. Thus, it is not a case of "uncharted territory" when it comes to such kind of provision.[108]

The Directive 95/46/EC[109] was conceived with concepts of the 1970's decade where card index boxes, punch cards and mainframe computers were the reality of information processing. In turn, nowadays the processing of data is "ubiquitous, global and networked"[110]. The information society has developed into a whole new dimension that reaches more stakeholders which increases the amount of data. In addition, the nature of the current Internet services complicates the identification of Controllers, Processors and Data Subjects, which are of extreme relevance to the data protection framework.[111] While the Directive remained applicable throughout the emergence of new technologies because of its technology neutral concepts and principles, such technological developments (admittedly positive for society) have endangered and increased the risks for privacy and data protection.[112] Therefore, the EU's data protection reform was motivated by the urgency to modernize the 1995 Data Protection Directive. The aim was to make the protections that it provisions more effective in the context of current times where technological turbulence and increasing global information flows of data are key factors.[113] According to the Article 29 Working Party report "*The Future of Privacy"*[114], the inclusion of the PbD principle in the new legal framework is as countermeasure to the effects of the threats mentioned. In the same report, it was suggested that the inclusion of the principle should concretize the general requirements into a broad and consistent principle and additionally recommended the adoption of regulations to cover specific technological contexts with PbD provisions for those contexts.[115]

The political leverage behind by these statements and the ones explored in Section 1.3, ultimately resulted in privacy by design being mandatory for data controllers[116] by result of the General Data Protection Regulation[117], commonly addressed as GDPR, being proposed in 2012. It went through several amendments and by December 2015 the Commission, Parliament and the Council completed negotiations. In early 2016, the final text was published and it provisions that the Regulation will come into force in 25th

[106] Directive 95/46/EC (Directive on protection of individuals with regard to the processing of personal data and on the free movement of such data).
[107] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
[108] Working Party (WP) Article 29 D-95/46/EC.2009. The Future of Privacy. 02356/09/EN-WP 168.
[109] Directive 95/46/EC (Directive on protection of individuals with regard to the processing of personal data and on the free movement of such data).
[110] Working Party (WP) Article 29 D-95/46/EC.2009. The Future of Privacy. 02356/09/EN-WP 168, page 12.
[111] Working Party (WP) Article 29 D-95/46/EC.2009. The Future of Privacy. 02356/09/EN-WP 168, page 12
[112] Working Party (WP) Article 29 D-95/46/EC.2009. The Future of Privacy. 02356/09/EN-WP 168.
[113] Easton C, 'Information Systems for Crisis Response and Management: The EU Data Protection Regulation, Privacy by Design and Certification' (Short Paper – Ethical, Legal and Social Issues Proceedings of the ISCRAM 2016 Conference – Rio de Janeiro, Brazil, May 2016 Tapia, Antunes, Bañuls, Moore and Porto de Albuquerque, eds.).
[114] Working Party (WP) Article 29 D-95/46/EC.2009. The Future of Privacy. 02356/09/EN-WP 168, page 13.
[115] Working Party (WP) Article 29 D-95/46/EC.2009. The Future of Privacy. 02356/09/EN-WP 168, page 13.
[116] Koops B.-J, Bodea G, Hoepman J-H, Leenes R, Vedder A, D3.4 Code as Code Assessment (VIRTUOSO FP7 project (2009).Lessig L, *Code: And other laws of Cyberspace* (3rd edn, Basic Books 1999).
[117] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

of May 2018. As stated above the 1995 Directive does not expressly mention the PbD principle, but the new Regulation contains several references. It is the first piece of legislation that explicitly mentions the principle and it can be regarded as an important step in the adoption of PbD due to the importance and impact of EU Law in Privacy and Data Protection.

In the case of the GDPR, the legislator chose to adapt the wording to "Data Protection by Design and by Default" revealing the European interpretation of Privacy by Design and its preference for the term "data protection" in order to be consistent with the European legal framework and its tradition. This is of course reflective of the European approach that considers privacy larger than data protection.[118] The differentiation between the right to privacy and the right to data protection in EU Law, namely in the EU Charter of Fundamental Rights[119], may also explain this choice of wording disregarding the international recognition of the term 'Privacy by Design'[120]. In article 25 (1) "Data protection by design" it is prescribed that:

> *"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."*[121]

As for data protection by default, article 25 (2) requires that:

> *"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*[122]

---

[118] Lachaud E, 'Could the CE marking be relevant to enforce privacy by design in the Internet of things?' in Serge Gutwirth, Ronald Leenes, and Paul De Hert (eds), Data Protection on the Move - Current Developments in ICT and privacy/Data Protection (Springer Science + Business Media 2016) 135–162; Hansen M, "Data Protection by Default in Identity-Related Applications" in Simone Fischer-Hübner, Elisabeth de Leeuw, and Chris Mitchell (eds), *Policies and Research in Identity Management: Third IFIP WG 11.6 Working Conference, IDMAN 2013* (2013).

[119] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, available at: http://www.refworld.org/docid/3ae6b3b70.html [accessed 3 June 2017]

[120] Tsormpatzoudi P, Coudert F, PRIPARE, Deliverable D5.1 State-of-Play: Current Practices and Solutions (2014). http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE_Deliverable_D5.1_v1.0.pdf

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

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

Additionally, article 25 paragraph 3 reads:

> *"An approved certification mechanism pursuant to article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article."*

Thus, the EU legislator took the approach of making Privacy by Design, albeit incorporated as it was deemed adequate, explicit in legislation. Obviously, where regulators will decide to adopt Privacy by Design, they will do so in whatever form or configuration (i.e relying on law-like approaches or simply relying in technology) they consider more adequate, because Privacy by Design is – as we saw in section 1.2 – an approach to privacy protection that has been developed and internationally acclaimed. PbD is in no way an "off-the-shelf" solution, nor a Treaty to adhere to, or meant to be incorporated in legislation by simply pasting Cavoukian's 7 foundational principles. The manner by which the approach can be adopted is, of course, flexible in the manner by which the regulator drafts the legislation (positive dimension of regulatory design) or chooses to adopt a law-like approach as a regulatory instrument and to combine it with the reliance on technology as regulation (normative dimension of regulatory design). In the same way as other regulatory fads or approaches have been adopted as they are formulated and gain popularity among regulators (e.g risk-based regulation), the approach to adopt PbD as a regulatory intervention may face a similar occurrence. However, these and other considerations ought to take place in the following chapters of this thesis, being that is this point is made only for sake of contextualization.

For now, it is sufficient to advance that the EU legislator chose to include the approach in legislation, by creating the principle of Data Protection by Design (and Default). Also noteworthy is that with this Privacy by Design to some extent and subject to interpretation of what that exactly entails is mandatory. As Gloria Fuster[123] described it, the EU right to data protection, consists of a triangular structure with three connected vertices that correspond to the obligations of data controller, the rights of data subjects, and the monitoring activities of independent Data Protection Authorities.[124] They are connected in the sense that e.g. the data controller has to comply with the duties prescribed by law in order to permit the data subjects to enjoy the rights granted to them. Thus, it is uncontroverted to state that the incorporation of the principle of data protection by design in recitals 78 and 108, and article 25, placed in the Chapter IV "Controller and Processor", in the section "General obligations" creates a legal obligation.[125]

Still on the EU law context, another example of incorporation of the PbD approach in regulation of Privacy and Data Protection is the expectation to have it included in the upcoming "Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications." It is for now a Proposal[126] and will replace the legislation commonly

[123] González Fuster G, 'Beyond the GDPR, above the GDPR' [2015] Internet Policy Review <http://policyreview.info/articles/news/beyond-gdpr-above-gdpr/385> accessed 7 August 2016.
[124] González Fuster G, 'Beyond the GDPR, above the GDPR' [2015] Internet Policy Review <http://policyreview.info/articles/news/beyond-gdpr-above-gdpr/385> accessed 7 August 2016.
[125] Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), *Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers*(Springer 2016) 199–212.
[126] DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)).

known as the ePrivacy Directive.[127] The approach is patent in the Proposal to the extent that by way of attempting to simplify the cookie rules, "it adopts a privacy by design approach".[128] There, it is proposed that consent or lack thereof to the use of cookies should be inferred from browser settings, placing the onus to collect consent and to provide users with cookie and tracking controls on the browser and software providers (consider e.g. OS providers of connected devices such as smartphones). Article 10 of the referred proposal reads: "Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end user or processing information already stored on that equipment."[129] Its second paragraph details that: "Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting."[130] Through this approach, the European Commission intends to centralize consent in software and move from the ineffective cookie banners and notices. More importantly, it places an obligation on the providers of software to accommodate for features that enable the end-user to control its privacy settings. This approach respects-user privacy, has default-settings envisioned and gives control to the user. Thus, it is very much a PbD approach.

1.5 Conclusion

The concept of PbD has matured from the contribution of many privacy experts from both technological and legal contexts. Ann Cavoukian, being the "most notable champion"[131] contributed a great deal to the dissemination of the approach that found its way into the European Data Protection framework and has achieved international recognition to the point that is being held as a gold standard in the privacy and data protection field. Currently, it must be understood as overarching concept that entails not only varied technological but also organisational aspects that aim for the enforcement of privacy and data protection principles in the context of the development of technologies, business practices and overall processes that carry processing of personal data or applications with privacy-invading potential.

The concept of PbD can be explained as what the principle entails, that is, in simple terms, that privacy and data protection safeguards should be embedded in whatever relevant proposition (product, process, service, system, etc.) in the early stages of development as a default. That is the core meaning of PbD and something to be adopted by every stakeholder when dealing with such propositions and applying the principle. But also, on a more high-level, it is a regulatory approach to tackle privacy and data protection

[127] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
[128] Brennan D, 'The E-Privacy Regulation – What's New?' http://www.algoodbody.com/insightspublications/the_eprivacy_regulation_whats_new accessed 12 June 2017.
[129] Article 10 of the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 10.1.2017 COM(2017) 10 final 2017/0003 (COD).
[130] Article 10 of the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 10.1.2017 COM(2017) 10 final 2017/0003 (COD).
[131] Koops B-J and Leenes R, 'Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law' (2013) 28(2) International Review of Law, Computers & Technology 159–171. DOI:10.1080/13600869.2013.801589

from a regulatory point of view. Adopting a regulation pursuant to PbD entails recognizing and facilitating the use of technology as a regulatory instrument to pursue Privacy and Data Protection goals, the promulgation of legislation and promoting and prescribing the adoption of Privacy by Design *modus operandi* as the former meaning advanced above details.

The origins of the concept are intrinsically connected with Privacy-Enhancing Technologies. However, being that the concept is currently broader than the mere deployment of those tools, the discussion at hand has to be treated with a more general scope that is more suited to assess the regulatory potential of PbD as whole. At the same time, the historical development of the concept and how the approach has been gradually embraced by policy-making shows that there is some momentum and optimism behind it. Its inclusion in the context of the GDPR - that is expected to bring the European Data Protection framework into the information society of the 21st century - also reveals the expectations placed on the approach.

Chapter 2: Regulatory effectiveness

2.1 Introduction

This chapter is aimed at exploring criteria for regulatory effectiveness. Specifically, it will focus on the criteria that are best fitted for assessing the regulatory effectiveness of Privacy by Design as enshrined in EU policy. This way, the chapter will answer the sub-question "What makes for effective regulation?" Firstly, the concept of Regulation is explored and defined in section 2.2. In section 2.3 regulatory effectiveness is generally explained. Section 2.4 takes a step further and highlights how different theories address regulatory effectiveness and its criteria. Finally, section 2.5 concludes with the criteria and theories best fitted to evaluate PbD - the Proposed Framework.

2.2 Regulation

The word "Regulation" can be found in different contexts, both legal and non-legal. In fact, the term has a number of different meanings[132], which makes it a problematic concept to construe in a clear and precise way as its very meaning and scope are still being debated and questioned.[133] In the context of this thesis it is not relevant to cover the whole debate or comprehensively address all the aspects. Instead, it is relevant to lay down the basic concepts, terminology and relevant aspects that will ultimately allow to better understand the criteria that informs regulatory effectiveness.

Having said that and even though there is no single concept of regulation in use found in the literature, it is fairly safe to describe it as having one main feature that is the attempt to modify or affect behaviour.[134] Commonly, this is achieved through the promulgation and enforcement of rules of behaviour.[135] This main feature is soundly coupled with what Selznick[136] claims to be "the 'central meaning' of regulation: a sustained and focused control exercised by a public agency over activities that are valued by a community".[137]

[132] Ogus AI, Regulation: Legal form and economic theory (Clarendon law series) (Clarendon Press 1994).
[133] Morgan B and Yeung K, *An introduction to law and regulation: Text and materials* (Cambridge University Press 2007).
[134] Vibert F, The new regulatory space: Reframing democratic governance (Edward Elgar Publishing 2014).
[135] Vibert F, The new regulatory space: Reframing democratic governance (Edward Elgar Publishing 2014).
[136] Noll R and Selznick P, 'Focusing Organizational Research of Regulation' in R Noll (ed), Regulatory Policy and the Social Sciences (1985) 363.
[137] Ogus AI, Regulation: Legal form and economic theory (Clarendon law series) (Clarendon Press 1994)**;** Selznick P, 'Focusing Organizational Research of Regulation' in R Noll (ed), Regulatory Policy and the Social Sciences (1985) 363.

However, there are other considerations at play as Vibert[138] explains. While Baldwin[139] and Black[140] highlight the aspect of modifying behaviour, Braithwaite[141] formulates this aspect differently by highlighting the aspect of steering and stating that regulation relates to steering flows of events. More importantly, other than the aspect of modifying behaviour, Baldwin et al.[142] advanced, the idea that regulation generally relates to three aspects that pursue that modification of behavior: "targeted rules, state interventions more generally and all mechanisms of social control by whomsoever exercised"[143]. This last meaning is a rather wider concept of regulation because it does not solely contemplate rules and state directions as regulation. Instead, it includes the idea that behaviour, or flows of events can be modified or steered by forces arising from other sources other than the state and the laws it enforces. Of course this more overarching concept is not the most commonly discussed. Actually, when for example someone refers to the fact that regulation hinders industry and innovation this rather concerns the "central meaning" mentioned above.[144]

For the purpose of this thesis, the broader concept is favoured. Firstly, it encompasses regulators other than the State or central government and secondly, it includes any mechanisms or tools that may have a regulatory effect, ranging from legislation to policies, international cooperation, architectural changes or self-regulation.[145] This is motivated by the fact that it welcomes all forms of social control, it includes intentional or unintentional mechanisms and irrespective of whether those are arising from the state or from any other actors. Julia Black refers to it as "decentred regulation"[146]. Accordingly, she claims that a "decentred analysis (…) opens up the cognitive frame of what 'regulation' is."[147] Thus, it provides a wider playfield to arrive at the desired conclusions of this thesis. As it does not limit what counts as "regulation" it prevents the situations that would render some considerations out of the scope of a regulatory effectiveness test. More importantly, it allows to consider a wider array of regulatory instruments and actors.

The literature on regulatory instruments is extensive and it has been explored in different disciplines, including law, economics, and public administration.[148] Rather than discussing the scope of regulation, it relates to the matter of how to regulate. In fact, said literature attempts to categorize the instruments according to different criteria (e.g. Yeung does so based on the instruments' 'underlying technique of control'.[149] More importantly, there is considerable literature that explores the choice of instruments and its

[138] Vibert F, The new regulatory space: Reframing democratic governance (Edward Elgar Publishing 2014).
[139] Baldwin R, Rules and government: Non-statutory rules and administrative law (Clarendon Press 1997).
[140] Black J, *Rules and regulators* (Oxford University Press 1997).
[141] Braithwaite J and Levi-Faur D, Regulatory capitalism: How it works, ideas for making it work better (Elgar, Edward Publishing 2008).
[142] Baldwin R, Hood C, and Scott C, *A reader on regulation* (Oxford University Press 1998).
[143] Vibert F, The new regulatory space: Reframing democratic governance (Edward Elgar Publishing 2014), page 13 (footnote 3).
[144] Ogus AI, Regulation: Legal form and economic theory (Clarendon law series) (Clarendon Press 1994).
[145] Biegel S, Beyond our control? Confronting the limits of our legal system in the age of cyberspace (MIT Press 2003) page xiv.
[146] Black, J. (n.d.). Critical Reflections on Regulation. Australian Journal of Legal Philosophy 27, pp.1-35, page 1.
[147] Black, J. (n.d.). Critical Reflections on Regulation. Australian Journal of Legal Philosophy 27, pp.1-35, page 1.
[148] Morgan B and Yeung K, *An introduction to law and regulation: Text and materials* (Cambridge University Press 2007), page 79.
[149] Morgan B and Yeung K, *An introduction to law and regulation: Text and materials* (Cambridge University Press 2007), page 79.

effectiveness in context.[150] For now, it suffices to mention this as in the following chapters we will discuss their characteristics, their choice and optimal combination. Namely, the ones employed in the regulation of PbD.

Regulation represents an important purpose in all contemporary societies from the international to the local level in all levels of organization.[151] The rules usually target businesses.[152] However, individual behaviour can also be targeted. Those rules may be set to influence behaviour in subtle ways, e.g. using market forces, such as a labelling scheme that inspires people to purchase from approved sources that guarantee that there was no involvement of child labour in the manufacturing of the product[153] - or maybe a labelling scheme that ensures consumers that privacy or data protection considerations are taken in a development of a product. On the other hand, rules can also be complemented by state sanctions, a not so subtle reminder that non-compliance will result in the sentencing to pay fines, sanctions or penalties[154] - such as the provisions on imposing administrative fines in the GDPR.[155] The motives behind regulating are very broad and can address various issues[156] ranging from the lack of use of seatbelts by drivers, unemployment or the environment. As another set of examples, consider the issues of lack of user knowledge on privacy settings, data subject's loss of control over data or citizen's privacy and data protection right as a whole.

The broad spectrum of issues addressed and the increasing penetration of regulatory activity in the "modern state" configuration, as documented in the literature, has led to an extensive debate about this activity that involves academics, regulators and the regulatees. One of the areas of the debate precisely concerns the effectiveness of regulation paired with the endeavour of measuring the performance of regulatory interventions once they have been promulgated. Usually, this assessment is made by comparing the performance of regulatory interventions against the proposed targets.[157] The statement and purpose of this thesis is not so far from this reasoning. However, as we will see in the remaining of the chapter, this method is not best suited to arrive at the conclusion.

2.3 Regulatory Effectiveness

The term "effectiveness" can be defined as the "degree to which objectives are achieved and the extent to which targeted problems are solved"[158] or "the degree to which something is successful in producing a desired result"[159]. It can also be formulated as "the ability to be successful and produce the

[150] See Grabosky P, Gunningham N and Sinclair D, *Smart Regulation: Designing Environmental Policy* (Oxford University Press 1998), Brownsword R, 'Code, Control, And Choice: Why East Is East And West Is West' (2005) 25 Legal Studies, Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008).
[151] Vibert F, The new regulatory space: Reframing democratic governance (Edward Elgar Publishing 2014).
[152] Vibert F, The new regulatory space: Reframing democratic governance (Edward Elgar Publishing 2014).
[153] Vibert F, The new regulatory space: Reframing democratic governance (Edward Elgar Publishing 2014).
[154] Vibert F, The new regulatory space: Reframing democratic governance (Edward Elgar Publishing 2014).
[155] See article 83, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[156] Vibert F, The new regulatory space: Reframing democratic governance (Edward Elgar Publishing 2014).
[157] Vibert F, The new regulatory space: Reframing democratic governance (Edward Elgar Publishing 2014).
[158] Business Dictionary, <http://www.businessdictionary.com/definition/effectiveness.html> accessed 28 November 2016.
[159] Oxford Dictionaries, <https://en.oxforddictionaries.com/definition/effectiveness> accessed 19 September 2016.

intended results"[160]. "Effectiveness" is assessed disregarding the costs and so it can be described as "doing the right thing"[161] towards a goal. In that sense it differs from "efficiency" which in turn translates to "doing the thing right"[162] and it is not included in the assessment of this thesis.

Connecting effectiveness to regulation, the notion of regulatory effectiveness requires some consideration. First of all, it is necessary to point out that the present discussion concerns "regulation broadly-understood"[163] as reflected in the previous section. Secondly, it is important to start by mentioning that regulatory effectiveness is where regulation achieves its purpose. As pointed out in the introductory chapter, broadly speaking a regulatory intervention will be effective if it succeeds in accomplishing the targeted regulatory objectives or standards.[164]

However, we cannot treat the present discussion in such terms. First, it is not a matter of whether a regulatory intervention is effective or not but rather how effective or ineffective it is.[165] Fukuyama believes that "no regulatory regime is fully leak-proof (...). [N]o law is ever fully enforced"[166] and he concludes that the fact that they are not was never a reason for dismissing a law or trying to enforce it.[167] Keeping in mind that the concept of regulation used in this thesis encompasses forms of regulation other than the classic use of legislation, it is important to point out that Fukuyama's reasoning is still valid even if a regulatory intervention is not backed by a law. Brownsword and Goodwin[168] have drawn from it and advanced the idea that where it comes to setting the bar for regulatory effectiveness, if the bar is set for full achievement, the only conclusion will be that "all regulatory interventions are ineffective"[169]. Following that reasoning, they suggest applying a "relative effectiveness and ineffectiveness" evaluation of a given regulatory intervention. It follows that effectiveness should not be accessed in absolute terms but rather evaluated in a matter of degree.[170] This way regulatory effectiveness is better tested in the sense of whether the regulatory intervention translates into an improvement when compared with the stated regulatory objectives. If the objective is to prevent a data breaches from occurring it is obvious that full regulatory effectiveness will be the occurrence of zero data breaches. On the other hand, if the objective is rather to encourage a conduct – e.g. to comply with the commands of specific principles as privacy by design - full regulatory effectiveness is not as clear. This is because it is practically impossible to detect levels of occurrence of

[160] Cambridge Dictionary, 'Effectiveness meaning in the Cambridge English dictionary' (23 November 2016) <http://dictionary.cambridge.org/dictionary/english/effectiveness> accessed 28 November 2016.
[161] Business Dictionary, <http://www.businessdictionary.com/definition/effectiveness.html> accessed 28 November 2016.
[162] Business Dictionary, <http://www.businessdictionary.com/definition/effectiveness.html> accessed 28 November 2016.
[163] Morgan B and Yeung K, An introduction to law and regulation: Text and materials (Cambridge University Press 2007).
[164] Brownsword PR and Goodwin M, Law and the technologies of the Twenty-First century: Text and materials (Cambridge University Press 2012).
[165] see Grabosky P, Gunningham N and Sinclair D, *Smart Regulation: Designing Environmental Policy* (Oxford University Press 1998), page 26.
[166] Fukuyama F, Our posthuman future: Consequences of the biotechnology revolution (Farrar, Straus and Giroux 2002).
[167] Fukuyama F, Our posthuman future: Consequences of the biotechnology revolution (Farrar, Straus and Giroux 2002).
[168] Brownsword PR and Goodwin M, Law and the technologies of the Twenty-First century: Text and materials (Cambridge University Press 2012).
[169] Brownsword PR and Goodwin M, Law and the technologies of the Twenty-First century: Text and materials (Cambridge University Press 2012).
[170] Brownsword PR and Goodwin M, Law and the technologies of the Twenty-First century: Text and materials (Cambridge University Press 2012).

such a conduct among the regulatees. On top of that, the regulatory intervention under assessment does not address such a simple problem as the example provided, which can be watered down to such binary outcome of an event occurring or not. The same goes for its objectives. In Brownsword and Goodwin[171] view, this further supports the choice of dropping absolute terms when gauging effectiveness and rather relying on a spectrum-like concept of regulatory effectiveness.[172]

Secondly, for the object at hand it more relevant to assess it from a regulatory design point of view instead of a performance perspective. Like Brownsword states: "when we assess the effectiveness of a regulatory intervention, we will tend to focus on matters of compliance and resistance, of correction and revision."[173] When doing the assessment *a posteriori*, and assuming there is a way to measure the level of occurrence/compliance, this makes complete sense. However, by merely judging the policy choices it is also possible to do it *a priori* (before tested in practice). This implies that the assessment can be performed in different phases (Browsword identifies three phases – direction, detection and correction[174]). As demonstrated by the sections below, it is possible to focus on criteria that relate to the regulation or policy design phase (or "direction"), as opposed to Brownsword's approach mentioned above. Therefore, it is not relevant for the present discussion to evaluate whether the regulation meets its objectives (performance/compliance perspective), but rather if the regulatory design meets the criteria of effectiveness in a manner that promises to enable their achievement (regulatory design perspective). The PbD principles were only recently included explicitly in EU Law – demonstrating a clear sign of the regulators adoption of the approach. The GDPR – where the approach was included in its provisions, thus providing the main object that allows for this assessment - is not yet in force. Thus, an assessment of effectiveness cannot be made by comparing objectives to results, because the results or the outcome of that regulatory intervention are not available yet. For these reasons, it is only logical that this thesis relies on the evaluation of the design rather than focusing on the levels of compliance. So the focus is on whether the regulatory intervention has been designed in an effective manner that allows to achieve those objectives. This can be achieved by crossing PbD policy choices with criteria or principles that inform effective regulatory design. Thus, this way, matters of compliance and enforcement (or 'detection' and 'correction' are put aside. Even though this is the case, the adoption of a spectrum-like analysis as advocated before for the *a posteriori analysis* is still valid. This is because an assessment of this nature also does not benefit from absolute terms as 'effective' or 'ineffective', but rather from an analysis in relative terms.

2.4 Criteria for Effective Regulatory Design

For the purpose of this thesis it is not relevant to discuss all criteria, but rather to select the ones that are best fitted to the object under assessment. In some cases, these criteria are more adequately described as principles or guidelines that inform effective regulatory design. The criteria found in the literature, even though in some cases designed to inform the regulation of specific contexts (e.g. Environmental law or cyberspace), provides for general considerations that can be extracted and provide

[171] Brownsword PR and Goodwin M, Law and the technologies of the Twenty-First century: Text and materials (Cambridge University Press 2012).
[172] Brownsword PR and Goodwin M, Law and the technologies of the Twenty-First century: Text and materials (Cambridge University Press 2012).
[173] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008).
[174] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008).

lessons for regulatory effectiveness in general. In the conclusion of this chapter, I advance my own framework that presents some criteria that follows the logic there explained.

2.4.1 Effective regulatory design and Regulatory Coherence

In "Designing Effective Regulation: A Normative Theory"[175], Sheehy and Feaver set out to determine whether the relationships between normative components of regulatory systems can determine the "design of more coherent and effective regulation" [176]. The main conclusion was that it is necessary to ensure regulatory coherence of regulatory systems (or, for the purpose of our argument, of regulatory interventions) in order to achieve effectiveness. Thus, a coherent regulatory design is an effective regulatory design.

In the context of discussing how to frame or select the policy response, Sheehy and Feaver's concluded that there was not much literature on the design of regulation since Breyer's[177] observation that regulators need to ensure that the problem (which the regulatory intervention seeks to address) must be in alignment with the method (that it is intended to achieve an objective).[178] They built on this reasoning and advanced that effective regulatory design is accomplished when the problem is coherently matched with the objectives, which in turn should be coherently matched with the approach.[179] Moreover, actors need to be defined as well in alignment with the components of the regulatory intervention.[180] This matching exercise is referred throughout their work as Regulatory Coherence.

Regulatory coherence concerns the fluid alignment of the components and processes of a regulatory system. Basically, for a regulatory intervention to be effective, in its design, the regulator must ensure that the relationship between the problem and the policy response to that problem is coherent.[181] Turning the principle around, the authors state that an incoherent normative regulatory framework is "a set up for failure".[182]

Regulatory coherence serves two purposes that can be leveraged by regulators. It informs the effective design of regulations and serves as a scheme for assessment. Thus, it can support in avoiding troubles in designing regulation such incoherence, fragmentation and generally the failure of the regulation.[183]

---

[175] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University of New South Wales Law Journal.*, 38(2), pp.395-425.
[176] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University of New South Wales Law Journal.*, 38(2), pp.395-425, page 393.
[177] Breyer S, *Regulation And Its Reform* (Harvard University Press 1984).
[178] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University ofNew South Wales Law Journal.*, 38(2), pp.395-425, page 410.
[179] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University ofNew South Wales Law Journal.*, 38(2), pp.395-425,Page 420.
[180] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University ofNew South Wales Law Journal.*, 38(2), pp.395-425.
[181] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University ofNew South Wales Law Journal.*, 38(2), pp.395-425, page 420.
[182] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University ofNew South Wales Law Journal.*, 38(2), pp.395-425.
[183] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University ofNew South Wales Law Journal.*, 38(2), pp.395-425, page 400.

2.4.2 Smart Regulation Theory

Smart Regulation theory was developed in the context of the heated debate between those who favoured a more regulatory state and those who in contrast argued for a less interventionist model of State.[184] More importantly, this theory provides guidelines for policy-makers to better design and choose their instruments and ultimately achieve their stated objectives.[185] It promotes a restrained government intervention by replacing it where adequate with alternative modes of regulation of public and private nature and/or market or non-market solutions.[186] Thus, this theory provides criteria for regulatory effectiveness as it informs "smart" regulatory tuning and choice of instruments that can be summed up in 8 principles as Van Gossum et al.[187] pointed out. For this thesis, the below were selected from that summary:

1. "choose policy mixes that incorporate a broad range of instruments"[188]

This criterion relates to the fact that regulators must realize the limitations of taking the approach of relying solely on a single regulatory instrument. In fact, the authors of the theory advanced that generally, those approaches are likely to be the least effective manner to address a problem through regulatory instruments.[189] Additionally, they state that generally, the effective alternative, is a multi-instrument approach that recognized the strengths and weaknesses of each individual instrument.[190] Moreover, the most effective way to capitalize on those strengths while accepting their weaknesses is through the use of complementary combinations of different instruments.[191] In conclusion, this principle relates to understanding the different instruments available and the contexts where their weaknesses and strengths will perform better.

2. "maximize opportunities for win-win outcomes."

This principle relates to importance of regulators capitalizing on possible incentives for regulatees to follow the behaviour modification intended. In order to do, regulators should identify and leverage scenarios where there is a benefit for the regulatees "burdened" by the regulatory effort in a way that ultimately will help to promote the goals of the regulation – the regulatee complies and reaps a benefit in balance with the burden and the regulator achieves the modification of the behaviour intended (win-win). Additionally, regulators should reward those regulatees who go beyond mere compliance and truly adhere

[184] Van Gossum P, Arts B, and Verheyen K, 'From 'smart regulation' to 'regulatory arrangements'' (2010) 43(3) Policy Sciences 245–261.
[185] Van Gossum P, Arts B, and Verheyen K, 'From 'smart regulation' to 'regulatory arrangements'' (2010) 43(3) Policy Sciences 245–261.
[186] Van Gossum P, Arts B, and Verheyen K, 'From 'smart regulation' to 'regulatory arrangements'' (2010) 43(3) Policy Sciences 245–261.
[187] Van Gossum P, Arts B, and Verheyen K, 'From 'smart regulation' to 'regulatory arrangements'' (2010) 43(3) Policy Sciences 245–261.
[188] Van Gossum P, Arts B, and Verheyen K, 'From 'smart regulation' to 'regulatory arrangements'' (2010) 43(3) Policy Sciences 245–261, page 247.
[189] Grabosky P, Gunningham N and Sinclair D, *Smart Regulation: Designing Environmental Policy* (Oxford University Press 1998.
[190] Grabosky P, Gunningham N and Sinclair D, *Smart Regulation: Designing Environmental Policy* (Oxford University Press 1998.
[191] Grabosky P, Gunningham N and Sinclair D, *Smart Regulation: Designing Environmental Policy* (Oxford University Press 1998.

to the desired behaviour.[192] Meaning that regulatees can act in a way where they only strive to be in technical compliance, which is not necessarily following the behaviour intended by the regulator. Thus, the regulation should be designed as to reward those who go beyond that mere technical compliance.

2.4.3 Biegel's "Basic Principles"

In Stuart Biegel's *Beyond Our Control?*[193] 20 basic principles are postulated in order to instruct the regulation of cyberspace. However, as the principles focus mostly on regulatory effectiveness,[194] it is possible to extract general lessons in the same way Brownsword did in "Rights, Regulation and the Technological Revolution", to inform the "regulation of modern technologies"[195] (whereas Biegel's aim is the "regulation of cyberspace"). In that regard, and as Brownsword also pointed out, it is possible to reconstruct Biegel's principles in a way that they inform general criteria for regulatory effectiveness as long as there is no distortion of the insights in those principles that are specific to a technology.[196] From the reinterpretation performed by Brownsword[197], the criteria selected for this thesis are as follows:[198]

1. "[Where] regulators [decide that a regulatory intervention is appropriate, they] should be clear about their objectives."

This criterion has direct connotation with both the regulatory coherence of components (one of them is the objectives component) and the one of the key processes identified in Smart Regulation theory that suggest that regulators identify the intended objectives of the regulation.[199] For this thesis, Biegel's formulation of the criteria was preferred, because it contains the requirement that objectives should be clear. These read together inform that Regulators should be clear about their objectives, because only then it is possible do perform regulatory design.

2. "Wherever possible, in setting their objectives, regulators should strive to build on consensus (regulate with the grain). Thus: a proposed regulatory approach may not be possible unless those that have the ability to resist agree to go along with the plan."

This criterion is connected to the second one of the previous section. They both relate to leveraging beneficial opportunities for the regulatees in order to make the regulation more likely to be followed. Or as

[192] Grabosky P, Gunningham N and Sinclair D, *Smart Regulation: Designing Environmental Policy* (Oxford University Press 1998.
[193] Biegel S, Beyond our control? Confronting the limits of our legal system in the age of cyberspace (MIT Press 2003) 359-64.
[194] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008).
[195] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008).
[196] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008).
[197] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008).
[198] Excerpts from Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008) and Biegel S, Beyond our control? Confronting the limits of our legal system in the age of cyberspace (MIT Press 2003) 359-64.
[199] Grabosky P, Gunningham N and Sinclair D, *Smart Regulation: Designing Environmental Policy* (Oxford University Press 1998.

Brownsword explained it, "regulators tend to better when they act with the backing of the regulatees".[200] Basically, regulators must identify factors of resistance to comply with the prescribed behaviour and seek to avoid defining goal that play into those factors. Turning it around, much like maximizing win-win scenarios, regulators should identify objectives that play into the interests of the regulatees.

3. "Regulators should consider the full range of regulatory instruments, from law-like interventions to strategies of self-regulation to code-based approaches."
4. "Regulators should also consider the optimal combination of regulatory instruments. Where problems are particularly intractable, there is no quick fix and regulators 'should identify combinations of approaches that may serve to move things in the right direction'[201]."

These criteria (4 and 5) correspond to the previous section criteria 1 and 2, but are differently formulated.

5. "Where regulators adopt a law-like approach, the standards should be 'clear, direct and understandable' and their requirements should be realistic."

This criterion relates to the situations where regulators define a command through means of legislation. In doing, that it should strive to understand what is a realistic standard to require and make it easy to understand and to adopt by the regulatees.

2.5 Conclusion: proposed effective regulation framework

<table>
<tr><td colspan="2">Framing</td><td>Problem</td><td>→</td><td>Objectives</td><td>Approach</td></tr>
<tr><td rowspan="3">Effective Regulatory Design</td><td rowspan="2">Underlying Criteria</td><td colspan="5">For a regulatory system to be normatively coherent, the relationship between the problem and the policy framing (in terms of objectives and approach) in response must be in alignment.</td></tr>
<tr><td>Identification of Problem Informs→</td><td rowspan="2">Policy Response</td><td>Definition of Objectives Informs→

In coherence with the problem</td><td>Design of the approach

In coherence with the problem and the objectives defined</td></tr>
<tr><td>Specific Criteria</td><td></td><td>Regulators should be clear about their objectives

Objectives should be defined along the consensus of the regulates

Maximize win-win outcomes</td><td>Regulators should consider the full range of regulatory instruments available and deploy their optimal combination;

Where resorting to law as a regulatory instrument, the standards should be 'clear, direct and understandable and their requirements should be realistic.</td></tr>
</table>

Table 1 – Proposed Framework.

All the criteria extracted and the reasoning that supports them are funded on basic logic assumptions. In a way, it seems that, when it comes to anything with regulating or designing effective regulation, one

[200] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008), page 137.
[200] Ayres I and Braithwaite J, *Responsive Regulation* (Oxford University Press 1992), page 148.
[201] Biegel S, Beyond our control? Confronting the limits of our legal system in the age of cyberspace (MIT Press 2003) 359-64.

must start (or should start) with basic reasoning. In fact, Brownsword stated that when it comes to regulatory effectiveness "there is no point in reinventing the wheel".[202]

Considering the object under assessment (PbD, as enshrined in EU Law) and the gap in the literature (evaluating PbD from an effective regulatory design perspective), I concluded that the criteria should mostly focus on the design of the policy (with emphasis on its normative dimension) while disregarding compliance or enforcement matters. Thus, dynamics between regulatees and regulatory agencies for example, and other governance dynamics which are more *a posteriori* components of regulation, such as Ayres and Braithwaite's 'responsive regulation'[203] are out of the scope of the present assessment. In fact, 'responsive regulation' is best described as an approach to enhance compliance through the improvement of the interactions between regulators and regulatees[204], which does fall in the scope of regulatory design.

This emphasis on the normative dimension of regulatory design, namely on the choice of instruments and the actors object of regulation is in line with the approach taken in the development of Smart Regulation theory[205]. The authors described their method as one focused in addressing the questions of regulatory strategy, and for each of them recommend guidelines for regulators to consider in designing successful environmental regulation.[206] Instead, the purpose of this thesis is to assess whether the PbD incorporation in EU Law observe criteria of effective regulatory design. According to Sheehy and Feaver[207], "the normative dimension [of regulatory design] (…) deals with theoretical and policy considerations determining the design of regulatory systems".

Neil Gunningham and Darren Sinclair, in their work on "Smart Regulation"[208] advance the idea that it is possible to build "a process and principle based framework". The Proposed Framework (see table 1) follows this idea as it consists of an Underlying Criteria that informs the design of the regulatory design process and prescribes principles for regulatory design throughout that process (Specific Criteria). The 'process' framework of this thesis follows Sheehy and Feaver's logic of components and the coherence as the Underlying Criteria.[209] Thus, the Proposed Framework (see table 1) is defined as a process that:

- Identifying the Problem;
- Coherently setting the Policy Response to that Problem,
- which consists of Objectives and Approach, that must be coherently align with each other.

This process part of the Proposed Framework will focus on those components of the regulatory design. By taking this approach, the effectiveness assessment obtains a more holistic perspective and

[202] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008), page 137.
[203] Ayres I and Braithwaite J, *Responsive Regulation* (Oxford University Press 1992).
[204] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University ofNew South Wales Law Journal.*, 38(2), pp.395-425,page 419-420.
[205] Grabosky P, Gunningham N and Sinclair D, *Smart Regulation: Designing Environmental Policy* (Oxford University Press 1998), page 22.
[206] Grabosky P, Gunningham N and Sinclair D, *Smart Regulation: Designing Environmental Policy* (Oxford University Press 1998), page 22.
[207] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University ofNew South Wales Law Journal.*, 38(2), pp.395-425.
[208] Grabosky P, Gunningham N and Sinclair D, *Smart Regulation: Designing Environmental Policy* (Oxford University Press 1998), page 375.
[209] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University ofNew South Wales Law Journal.*, 38(2), pp.395-425.

follows a logical procedure. To enrich that underlying reasoning, the Specific Criteria are leveraged to deepen the analysis and address certain matters that not only are important in the design of regulatory interventions, but are also fit to the specific characteristics of PbD. The Specific Criteria selected from the literature (those in the previous section) are matched to those components/process.

Having the Proposed Framework defined as such, it allows to evaluate PbD as enshrined in EU Law. The GDPR's provisions and the literature discussing the adoption of the PbD approach (both in that legislation and in EU policy) serve as reference for the assessment.

Chapter 3: Proposed Regulatory Effectiveness Framework applied to Privacy by Design

3.1 Introduction

In the previous chapter I presented the Proposed Framework that intends to test the object against the proposed criteria. This chapter brings together the object of the assessment – that is PbD as enshrined in EU Law – together with the Proposed Framework. In 3.2 the problem that the European regulator intends to tackle by adopting the PbD approach is discussed. In 3.3 the process by which the problem is translated into a regulatory response is explained - 3.4 and 3.5 correspond to the two aspects of that response (objectives and approach). In 3.5 the assessment will then focus on first, identifying the instruments that Privacy by Design leverages and after to understand the full range of available instruments and their optimal combinations and evaluate whether PbD is effectively designed with regards to the choice of instruments. The same goes for 3.6 but with regard to the targets of the regulation.

PbD is a regulatory approach that, among other things, promotes the employment of techno-regulation as an instrument/modality to achieve the general goals of privacy and data protection laws. By prescribing this particular strategy, it can be understood a regulatory approach to Privacy and Data Protection. This means that PbD has some intrinsic characteristics that are already product of normative choices by their original developers (for example, when discussing it, one cannot ignore that techno-regulation component).At the same time it can take a number of forms, when being adopted by regulators These possible forms or variations are product of different normative choices. Such is the case of the EU regulator, that, as pointed out in Chapter 1, decided e.g. to make it explicit in the law (choice of instrument) and coupled it with a certification mechanism. The assessment performed in this chapter will have this as the object. When analysing the effectiveness of its regulatory design it can conclude for different choices as well. Namely, where the coherence test or the application of the criteria will so suggest.

3.2 Problem

The Problem PbD attempts to tackle is the manner by which phenomena's that are harmful to privacy and data protection are primarily dealt. In fact, the manner by which they are dealt is characterised by being reactive and consequently insufficient in protecting data subjects' rights and over-burdening organisations and consequently hindering innovation with ineffective protection to privacy and data protection. Part of the problem is that these protections are exactly reactive in nature, and more importantly, they react and adapt slowly and in a remedial manner when the damage is already made.

That major dimension of the problem is underlined by other troublesome aspects. First, the fact that personal data has become an important and valuable asset for organisations.[210] This applies both for business (e.g. monetization of data through digital services or insights) or government and public bodies (e.g. for pursuing benefits for society such as national security or Big Data initiatives) and is made worst by the general public's lack awareness of the risks it entails. The extraction of value from data is made

[210] Koops B, 'The trouble with European data protection law' (2014) 4(4) International Data Privacy Law accessed 20 December 2015 250–261.

possible by both technology and services developed over recent years and how processing of personal data is transversal to many aspects of daily-life. In fact, such technology (and how fast it develops) is another aspect of the problem. The technological turbulence currently witnessed enables the phenomena mentioned and increases the dimension of the risks. In fact, they are facilitated by the alarmingly fast growing automatic processing of information and its cheap storage in databases. These rapid technological developments such as Artificial Intelligence, Big Data, Clod computing and services and products that leverage these and other technologies) allow for the automatic processing of incredible sums of data from various interconnected sources in a ubiquitous manner and knows no borders. As a matter of fact, transnational data processing challenges the enforcement of regulation and consists of yet another aspect of the wider problem that PbD tries to approach. In fact, generally speaking Privacy and Data Protection jurisdictions around the globe share problems due to the current data processing that easily overreaches national boundaries.[211]

This reality represents an increase of risks of privacy and data protection rights violations.[212] Additionally, it has been claimed that recent this scenario may have rendered global legal frameworks (and even the principles of privacy) inadequate.[213] Mainly, this is motivated by the major problem mentioned above - risks tackled in a way where technology is adapted to mitigate the problems after they come to light and when the damage is already done.[214] This is explained by the fact that for example, those technologies – often referred to as Privacy Invading-Technologies (PITs) – are being developed and embraced at a pace that regulation cannot keep up with. Hence why they are often described as "disruptive". More importantly, designers, developers and producers are generally not targeted by privacy and data protection measures and regulation, which greatly contributes to the problem. This results in law and regulation being, as Klitou puts it, "behind the advancement of technology"[215]. In line with this reasoning, it has been advanced that the adoption of the GDPR is made in the context of EU Data protection laws trying to step up to the challenges arising from that technological turbulence.[216] All these reasons explain why it is important to consider privacy and data protection in advance so those issues and risks can be prevented in the first place – this is the reasoning of PbD.

The first step to test the effective regulatory design of Privacy by Design is to identify the problem in its genesis. In identifying a Problem, first, a given social practice or activity that has some sort of social effect has to be noticed by the community. This is something that takes place long before the regulatory activity even begins.[217] Then it inspires the first decision that has to take place, which is whether such social effects deserve attention. Not all social effects will be considered a problem, because they are influenced by cultural and cognitive factors and in fact, the perception of the problem is not something obvious or

[211] Bennet, C and Raab, C, 'The Governance of Privacy: Privacy Instruments in global perspective' (2003), page 196.
[212] Viola de Azevedo Cunha M, *Market integration through data protection: An analysis of the insurance and financial industries in the EU* (Springer 2013) page 3-4.
[213] Klitou D, 'Privacy by design and privacy-invading technologies: Safeguarding privacy, liberty and security in the 21st century' (2011) 5(3) Legisprudence 297–329, page 298.
[214] Krebs D, ''Privacy by Design': Nice-to-Have or a Necessary Principle of Data Protection Law?' (2013) Vol. 4, 2013 JIPITEC.
[215] Klitou D, 'Privacy by design and privacy-invading technologies: Safeguarding privacy, liberty and security in the 21st century' (2011) 5(3) Legisprudence 297–329, page 297.
[216] Easton C, 'Information Systems for Crisis Response and Management: The EU Data Protection Regulation, Privacy by Design and Certification' (Short Paper – Ethical, Legal and Social Issues Proceedings of the ISCRAM 2016 Conference – Rio de Janeiro, Brazil, May 2016 Tapia, Antunes, Bañuls, Moore and Porto de Albuquerque, eds.)
[217] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University of New South Wales Law Journal.*, 38(2), pp.395-425, page 403.

evident.[218] Thus, the problem needs first to be deemed as having normative implications that deserve a regulatory intervention. In fact, even though it is in the Proposed Framework, one of the ideas gathered was that regulators should start by considering "Whether the regulatory intervention is needed in the first place". Furthermore, when identifying a "problem" one should not assume that it is something harmful. It can be that the perceived social activity generates some benefit that is not fully leveraged and that is the problem to be addressed.[219]

In the context of identifying problems, Sheevy and Feaver considered the problem identification from a "socio-psychological approach"[220], which instead of simply looking at problems as facts it rather considers the social facts as either social practices or social effects.[221] A social practice can be simply defined as the behaviour of the actors relevant for the context at hand. In the same way, a social effect can be defined as the result of those behaviours on society. They concluded that when considering social practices and social effects, regulation's object should be the social practices, in order to change social effects.[222] This reasoning deserves due consideration from a regulatory design perspective as it has fundamental implications. Moreover, one important challenge is scarce information about the nature of the problem.[223]

The Problem as a regulatory component is where the first problems arise in the design of effective regulation. If it is broken down into the normative decision it entails – whether the Problem deserves to be addressed by regulation and its characterisation – two problems in the regulatory activity arise. First, it can be ignored when it deserves to be addressed or the other way around, it is a Problem that rather should be left alone and thus an omission by the regulator is the best option. Secondly, it can be poorly characterised and lead to an inappropriate response, or the characterisation is not coherent with the response (the latter it is a failure in defining the policy response rather than characterising the problem).

Applying the method presented above and having identified the PbD's "Problem", it is safe to advance that, as seen in 1.4, the European regulator found the problem worth regulating and with regards to that there is no space for challenging that first regulatory decision (as advanced in the Introduction and Chapter 1). Then, it is useful to consider the current use of Privacy Invading Technologies and the volume and manner by which personal data are processed. Then consider their impact in society. Respectively, these are the social practices and the social effects in Sheevy and Feaver's reasoning and that are subject to the assessment at hand. It is arguable that privacy regulation should tackle those social practices instead of its effects. Thus, the result is that regulation should (at least *effective* regulation) focus on the development

[218] "Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University ofNew South Wales Law Journal.*, 38(2), pp.395-425, page 394; Holland D and Quinn N, 'Culture And Cognition', Cultural Models in Language and Thought (Cambridge University Press 1987).
[219] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University ofNew South Wales Law Journal.*, 38(2), pp.395-425, page 402.
[220] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University ofNew South Wales Law Journal.*, 38(2), pp.395-425, page 395.
[221] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University ofNew South Wales Law Journal.*, 38(2), pp.395-425, page 395.
[222] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University ofNew South Wales Law Journal.*, 38(2), pp.395-425, page 396.
[223] Organisation for Economic Co-operation and Development. Public Management Committee,OECD working papers: Reducing the risk of policy failure: challenges for regulatory compliance : 21st Session of the Public Management Committee, Château de la Muette, Paris 6-7 April 2000.

of the PITs and the dimension and volatility of current processing activities as defined above. This means that instead of focusing on the consequential social effects, regulation should focus on their source – the social practices. Conversely, PbD should focus on the design of the technologies, services and products in on hand, and on the practices on the other. The following sections – namely the Objectives and Approach – will serve to assess whether the problem as defined is there coherently aligned.

Another matter is the fact that PbD can arguably be seen as a regulation that taps into an opportunity as well. Consider the reasoning of Cavoukian, which believes that when applied, the principle allows "for greater privacy (...) while enabling organizations to gain a competitive advantage that is sustainable over time".[224] Thus, as seen above, PbD as a regulatory approach seeks to address a social issue arising from social practices that are problematic, but it can be partly framed as an approach that taps in an opportunity not explored by society. What Cavoukian suggests is that when those who are targeted by regulation adopt compliant data processing and design of technology it creates a benefit for them (explained by consumer trust and business management benefits from good data processing practices). If the Problem is framed as to mean that this benefit is not being fully leveraged by society then the regulatory problem gains another dimension that seems to provide a more rich regulatory design. This way the regulation will have also an opportunity dimension to it.

In conclusion, the problem as states above was gathered from the literature and serves perfectly as the reference of coherence that needs to be achieved in the rest of the components of the regulation. This includes, the opportunity/benefit aspect of it. It makes sense that while a regulatory intervention is seeking to alter the social practice the regulator might as well make it an opportunity. This reasoning is explored in 3.4, but it is important that the Problem characterised as having an opportunity to tap in by the actors of the regulation should have a coherent throughout the Policy Response. Furthermore, having the problem as defined above will greatly improve the odds to achieve more coherent results in the Policy Response. In the following sections this is considered.

3.3 Policy Response (Objectives and Approach)

The policy response is the regulatory intervention that seeks to address the Problem. "Policy", as defined by Jenkins[225], refers to a group of connected decisions by a regulator with regards to the choice of objectives and methods to accomplish them within a given context. The Policy Response, as conceptualized by Feaver and Sheevy, comprises two regulatory components: the Objectives and the Approach.[226] The Proposed Framework advanced in this thesis subscribes to this formulation.

[224] Easton C, 'Information Systems for Crisis Response and Management: The EU Data Protection Regulation, Privacy by Design and Certification' (Short Paper – Ethical, Legal and Social Issues Proceedings of the ISCRAM 2016 Conference – Rio de Janeiro, Brazil, May 2016 Tapia, Antunes, Bañuls, Moore and Porto de Albuquerque, eds.).
[225] W I Jenkins, Policy Analysis: A Political and Organizational Perspective (St Martin's Press, 1978) 15; Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University of New South Wales Law Journal*, 38(2), pp.395-425, page 410.
[226] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University of New South Wales Law Journal*, 38(2), pp.395-425.

The Policy Response starts with translating a Problem into regulation through the regulatory design process.[227] The Problem that PbD seeks to address and the Policy Response it prescribes must be coherent. In fact, where the Problem and the Objectives are not in alignment, the consequence can be that the regulator will define the wrong Objectives, fail to focus on the right actors and targets and leverage the wrong instruments, which leads to ineffective regulation.

Then, the focus is on the Approach. Policy literature describes the approach as the method employed to accomplish the policy objectives.[228] Thus, where in the Objectives the discussion concerned is identifying collective goals of the regulatory intervention, the Approach deals with "questions of mechanics and questions concerning how to regulate."[229] There are different influential factors, such as ideological, political and following intellectual fashions, that determine the choice of approach.[230] Designing this regulatory component is a crucial step in the design of the regulation as coherent so highly aligned links must be put in place between it and the Problem and Objectives of the regulation. Naturally, this is a point where incoherent decisions can easily occur in the regulatory design.[231]

In the way the Proposed Framework was structured, the Approach focuses on two aspects. Hence, PbD's Approach will be tested on the Instruments it relies on to pursue its objectives and tackle the Problem and the Targets of the regulation.

3.4 Objectives

3.4.1 Regulators should be clear about their objectives

As mentioned, one of the first action in developing the Policy Response is to explicitly define the Objectives. Objectives relate to the desired outcomes of the regulation – what the regulation wants to accomplish.[232] Concerning the regulatory component of Objectives, one of the attached Specific Criteria in the Proposed Framework is that regulators should be clear about their objectives. This criterion is heavily based on the extraction of Biegel's principles by Brownsword.[233] However, it is also picked up in Smart Regulation[234], where the authors state that identifying the desired policy objectives is essential. This criteria reasons with the idea of coherence, because a regulator cannot effectively match the objectives to the other regulatory components if they are not clearly defined in the first place. Basically, the vessels of the regulation must be all facing the same direction if it is to arrive at the desired destination.

---

[227] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University of New South Wales Law Journal*, 38(2), pp.395-425, page 413.
Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University of New South Wales Law Journal*, 38(2), pp.395-425, page 417.
[229] Morgan B and Yeung K, An introduction to law and regulation: Text and materials (Cambridge University Press 2007), page 79.
[230] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University of New South Wales Law Journal*, 38(2), pp.395-425, page 418.
[231] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University of New South Wales Law Journal*, 38(2), pp.395-425, page 417.
[232] Sheehy, B. and Feaver, D. (2015). Designing Effective Regulation: A Normative Theory. *University of New South Wales Law Journal*, 38(2), pp.395-425, page 413.
[233] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008) page 147.
[234] Grabosky P, Gunningham N and Sinclair D, *Smart Regulation: Designing Environmental Policy* (Oxford University Press 1998), page 380.

A number of vague and multiple policy objectives can be identified throughout the Privacy and Data Protection systems and they can be interpreted in many different ways such is their vagueness and level of abstraction. For example, Bennet and Raab claim that in order to evaluate the effectiveness and other qualities of Privacy and Data Protection in general, the goals to consider are "Protecting Privacy", "Promoting Good Computing Practice" and a "Balance Between the two."[235] Since the present focus is on EU Law, the general objectives of the GDPR can be considered as well - to reinforce data protection rights of individuals, ease the free flow of personal data in the digital single market, namely through the reduction of the administrative burden.[236]

However, since we are focusing specifically in the adoption of PbD in EU policy, the emphasis of the test should be in its particular goals. The developer of PbD, defined the goals of the approach as "ensuring privacy, gaining control over one's information, and, for organizations, gaining a sustainable competitive advantage." [237] The objective of ensuring privacy (and similar phrasings) are not specific to the approach and to the problem it tries to address. However, it needs to be pointed out that this obviously needs to be considered by the regulator when framing the approach. Namely, it needs to be considered which instruments and which target regulatees will achieve the assurance of privacy. Going back to the "clear" criteria, it should be said that "privacy" is not only vague as it is subjective.[238] Meaning that privacy, as mentioned in the Introduction Chapter of this thesis, is privacy is a troublesome concept to define. This is especially the case if the numerous applications of PbD are considered and the different results that can be achieved. Moreover, this is in line with Spiekermann's claim that privacy as a concept is not clear enough for it to allow regulators to know exactly what to protect.[239] Thus, in this regard the conclusion is that the definition of a clearer objective of ensuring privacy should be determined contextually. In fact, it is better dealt with in the definition of the positive dimension of the PbD regulation in the EU (which is out of the scope of this thesis). From an effective normative regulatory design perspective, ensuring privacy should definitely consist of one of the Objectives.

In comparison "gaining control over one's data", it is an objective slightly more straightforward because it dictates one way to ensure data subjects' privacy – by gaining control of how and to what extent data concerning them is processed. Moreover, since the approach of PbD is, for example, characterised by default settings that mechanically allow for preservation of privacy without additional actions, this objective must be argued for. For sake of coherence between the instruments defined in the approach and the objectives, it should be part of the regulators' roster of goals.

More importantly, one objective that is not so clearly identified by the legislator when interpreting the PbD provisions in the GDPR, is the shift of paradigm that reverts the reactive manner that has characterised the method through which EU Privacy and Data Protection policy can be characterised. Again,

[235] Bennet, C and Raab, C, 'The Governance of Privacy: Privacy Instruments in global perspective' (2003), page 191-3.
[236] 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, Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD).
[237] Cavoukian A, '7 Foundational principles' (August 2009), page 2.
[238] Bennet, C and Raab, C, 'The Governance of Privacy: Privacy Instruments in global perspective' (2003), page 197.
[239] Spiekermann, S, The challenges of privacy by design. Commun. ACM 55(7)(2012), 38-40.

for the sake of coherence between the regulatory components (this problem was raised in 3.2) and the approach, the regulators objectives must contain this rationale and it must be reflected in the rest of the regulatory design. Additionally, as we will see in the next section, the regulator must define one of Cavoukian's objectives (see 1.2). That is the goal to enable organisations in gaining a competitive advantage through PbD. This is explained in the next section.

In conclusion, PbD's objectives, if formulated as discussed can be considered "clear". More importantly, defined as such, they are set for coherence across the regulatory design. Even though the objectives are not easily advanced here, it is worth mentioning that the ones advanced meet that Specific Criteria, because they are specific and direct and not vague and subjective as e.g. ensuring privacy.

3.4.2 Objectives defined in line with the regulatee's consensus – regulatee resistance

In the Proposed Framework, one criterion suggests that in defining the objectives, regulators should attempt to do it by playing into the acceptance and interests of the regulatee. The reasoning employed is that by embedding in the regulatory design objectives that are aligned with the regulatees interests, there will be less resistance by those who have to comply, making the regulation more fit for effectiveness. Simply put, effective regulation can be better accomplished where the norms designed are backed-up by regulatees.[240] This criteria is connected to the notion of regulatee resistance (that can be of economic, cultural, professional, or moral nature).[241]

For example, the default settings, something very much in line with the PbD approach, whereby users do not need to take any action to protect their privacy, is something that finds resistance in many industry circles as it entails an opt-in approach for the collection of personal data to take place in the first place, which is something completely contrary to business interests and practices.[242] This needs to be balanced out in the regulatory design by providing regulatees with incentives, benefits for them to adopt the desired behaviour.

Additionally, this is somewhat connected with the criteria that regulators should maximize win-win opportunities (see 2.4.2). Meaning that where a regulation has the potential to provide scenarios where stakeholders with obligations can reap some benefits (creating a mutually beneficial situation for regulator and regulatee), those scenarios have to be leveraged to their full extent in order to provide for effective regulation.

For example, consider one of PbD's Objectives, which is for organisations to gain a sustainable competitive advantage. In Cavoukian's model of PbD this is the objective that can be evaluated against this

[240] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008), page 148.
[241] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008), page 148.
[242] Davies S, 'Why privacy by design is the next crucial step for privacy protection' [2010], http://i-comp.org/wp-content/uploads/2013/07/privacy-by-design.pdf accessed 14 October 2016, page 3.

criteria. She believes that organisations can leverage privacy to their own interests.[243] Let us remember that Cavoukian formulated PbD as an approach to be put in practice at an organisational level.[244]

The normative choice of emphasizing this advantage in complying with PbD translates into one objective being defined "with the grain" by the regulators. In this case, Cavoukian seems to suggest that regulators promotes a purpose that is in line with the interests (economic incentive) of those that are in a position to resist complying with the regulation. This is important because, as it will be demonstrated, economics are influential in the adoption of PbD practices and PETs.[245]

However, there are other factors that can be motivators for the compliance with PbD provisions as they create consensus with the regulatee. As Cavoukian[246] states, businesses that comply with PbD, can benefit from:

- "competitive advantage in the marketplace against businesses that do not offer privacy-respecting products or services or do not handle personal data respecting consumer or costumer personal data;" [247]
- "consumer trust and loyalty"; [248]
- "process efficiency and mitigation of risks as a result of processing merely the personal data needed for the business purposes;" [249]
- "Minimisation of risks and, as a result, costs related to privacy breaches."[250]
- "Reduction of costs in addressing privacy by taking a proactive posture in the implementation and development of privacy compliant products and services, rather than trying to remediate privacy-related constrains with increased resources spending;"[251]

To argue for the merit of this reasoning, Cavoukian advanced the idea that consumers are already turning privacy into a business issue rather than a compliance issue. This is explained by the fact that market (consumers) are starting to incentivizes that products and services are developed in compliance with Privacy and Data Protection, which the consumers see as an added-value. In fact, she believes that when applied

[243] Cavoukian A, 'Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers' [2011]
[244] Cavoukian A, 'Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers' [2011] <https://privacybydesign.ca/content/uploads/2011/08/pbd-law-policy.pdf> accessed 12 November 2015.
[245] Rubinstein, Ira, Regulating Privacy by Design (May 10, 2011). Berkeley Technology Law Journal, Vol. 26, p. 1409, 2012. Available at SSRN: http://ssrn.com/abstract=1837862
[246] Cavoukian A, 'Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers' [2011]
[247] Cavoukian A, 'Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers' [2011]
[248] Cavoukian A, 'Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers' [2011]
[249] Cavoukian A, 'Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers' [2011]
[250] Cavoukian A, 'Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers' [2011]
[251] Cavoukian A, 'Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers' [2011]

the principle allows "for greater privacy (...) while enabling organizations to gain a competitive advantage, that is sustainable over time".[252]

Moreover, J. van Rest et al.[253] posit that if "individual and collective privacy interests would be aligned with economic interests then our economic interests would also stimulate privacy". However, this market mechanism argument is sabotaged by a study presented by J. van Rest et al. that concludes that individual citizens (understood as consumers, customers or users) do not necessarily prefer products or services that protect their privacy.[254] Furthermore, the appearance of PbD in the first place exposes the threats of the increasing collection of data by private and public agents combined with the staggering user's deficit of consciousness concerning the advantages of privacy protecting technologies.[255]

Where regulatees do not back the regulation and adopt the same rational and economical perspective, they will perceive it as a cost for a certain behaviour. Applying this rationale to PbD, a regulatee may simply perceive it as a burden translated in material costs, associated with investment in compliance for example. Brownsword suggests that one outcome of economic resistance, is that when the behaviour prescribed by the regulation is perceived purely from a rational and economic perspective, the regulatee may find that non-compliance is the cheapest option.[256]

Furthermore, another relevant aspect is the fact that "Regulatees who truly internalize the regulations and their purpose will outperform regulatees who mechanically apply the prescribed standards."[257] This is very much connected to the criteria advanced – regulations with objectives defined as an incentive for the regulatees allows for the meaningful adoption of the prescribed behaviour as opposed to regulatees merely complying with the regulation. If regulatees have an actual interest in complying, then they will really be predisposed to actually "go with the plan" and adopt the regulators desired conduct, not only trying avoid the consequences of non-compliance.

The PbD approach encourages a focus not on mere technical compliance, but rather on approaching privacy holistically, as a design feature of an entire organization's activities and processes, embedding respect for privacy in a meaningful manner in order to obtain a high privacy standards[258], which is very much compatible with argument of internalization of regulation.

---

[252] Easton C, 'Information Systems for Crisis Response and Management: The EU Data Protection Regulation, Privacy by Design and Certification' (Short Paper – Ethical, Legal and Social Issues Proceedings of the ISCRAM 2016 Conference – Rio de Janeiro, Brazil, May 2016 Tapia, Antunes, Bañuls, Moore and Porto de Albuquerque, eds.).
[253] van Rest J and others, 'Designing Privacy-by-Design' in B Preneel and D Ikonomou (eds), Privacy Technologies and Policy - First Annual Privacy Forum, APF 2012 Limassol, Cyprus, October 2012 Revised Selected Papers(2014).
[254] van Rest J and others, 'Designing Privacy-by-Design' in B Preneel and D Ikonomou (eds), Privacy Technologies and Policy - First Annual Privacy Forum, APF 2012 Limassol, Cyprus, October 2012 Revised Selected Papers(2014).
[255] Easton C, 'Information Systems for Crisis Response and Management: The EU Data Protection Regulation, Privacy by Design and Certification' (Short Paper – Ethical, Legal and Social Issues Proceedings of the ISCRAM 2016 Conference – Rio de Janeiro, Brazil, May 2016 Tapia, Antunes, Bañuls, Moore and Porto de Albuquerque, eds.).
[256] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008), page 148.
[257] Brownsword R, Rights, regulation, and the technological revolution (Oxford University Press 2008).
[258] Cavoukian A, 'Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers' [2011] <https://privacybydesign.ca/content/uploads/2011/08/pbd-law-policy.pdf> accessed 12 November 2015.

P. Tsormpatzoudi et al,[259] while elaborating on implementation challenges of PbD, pertinently pointed out that when developing technologies mere legal compliance can result in "legal workarounds" that only take place because of compliance risks. An example is provided where according to the PbD obligation data minimization measures of whatever nature are put in place but the collection of personal data is not necessary altogether. Because of this scenario, it is stated that the privacy preservation should be "a goal in itself in product development". Rather than mere compliance, PbD must be part of the working culture and decision-making in an organisation.[260] Koops and Leenes[261] also agree on this point and find that the ones who employ data processing systems and the ones who develop them must internalise the data protection framework and accordingly, design those systems on the basis of PbD.

In conclusion, while a PbD regulatory intervention will benefit from defining objectives in line with the consensus of the regulatee, those benefits are somewhat questioned. In turn, this may influence the effects that this regulatory emphasis on the advantages of complying with PbD has on the outcome of the regulation. However, a PbD regulatory intervention (such as Cavoukian's model) that emphasizes benefits for compliance to its targets will be a more effective one. Therefore, leveraging this rationale is fundamental for the effectiveness of the regulatory design. Even though it is not noticeable from the information available, it is important that the EU Regulator, through a way or another, makes this benefits clear for the regulatee so that they can align their interests to those of the regulation. Informative regulatory instruments can perform well in achieving this.

3.5 Approach - Instruments

With regards to instruments, the Proposed Framework advances two related Specific Criteria which, read together, postulate that regulators should consider the full range of available instruments and strive to deploy their optimal combination effectively leveraging each of their strengths. Koops, while evaluating the state of EU Data Protection Law, presented some valuable insights for the present discussion. For example, he highlighted the poor choice of relying in command and control law and at the same time ignoring other regulatory instruments available to the regulator.[262] Privacy and Data Protection regulations are by no means restricted to legislation and legal mechanisms.[263] Neither is PbD.

In order to understand the different instruments, it is helpful to make use of Yeung's[264] systematization by the instruments' "underlying modality". The modality of the instruments is the

[259] Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers(Springer 2016) 199–212;
[260] Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers(Springer 2016) 199–212;
[261] Koops B-J and Leenes R, 'Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law' (2013) 28(2) International Review of Law, Computers & Technology 159–171. DOI:10.1080/13600869.2013.801589
[262] Koops B, 'The trouble with European data protection law' (2014) 4(4) International Data Privacy Law accessed 20 December 2015 250–261.
[263] Bennet, C and Raab, C, 'The Governance of Privacy: Privacy Instruments in global perspective' (2003), page 95.
[264] Morgan B and Yeung K, *An introduction to law and regulation: Text and materials* (Cambridge University Press 2007).

mechanism through which a given behaviour is regulated. It follows that behaviour can be controlled by command, competition, consensus, communication and code (or architecture).

This is by no means an exhaustive and complete overview, but serves as a base of understanding for the following discussion. To begin with, command based mechanisms are the typical regulatory instrument that are characterised by the prescription of legal rules associated with penalties. They are commonly known as 'command and control' or 'classical' regulation;[265] Consensus, known for its most popular tool 'self-regulation', leverages cooperation as the tool for the regulation of a certain behaviour and its distinct trait is the consent of the stakeholders.[266] In turn, communication based mechanisms are those which rely on the interaction with actors and targets of a given regulation (or even indirectly concerned with it) to educate and persuade them in order to fulfil the regulatory purposes.[267] Finally, code, also known as techno regulation or referred to as architecture, is the regulatory instrument that disregards human decision with regards to its behaviour by mandating a certain conduct through the 'designing-out' non-compliance.[268]

In order to consider the whether the regulator consider the full range of available regulatory instruments it is relevant to consider which ones were employed. In 3.5.4 considerations are made to that consideration and the optimal instrument combination. The linkages between all the instruments employed is what characterises a regulatory system or intervention. [269] Thus, Privacy by Design can be characterised (in part) by the instruments employed and the connection between them. Klitou states that PbD is a "critical combination of technology and law".[270] This means it is a combination of technological design (architecture, or code) and legal solutions. In EU law, the regulator took the following approach:

a) decided to make it explicit in the law (GDPR art.25);
b) included a certification mechanism and codes of conduct(self-regulation) pursuant to art. 25 (GDPR art.25 paragraph 3, 40, 42);
c) code aspect is derivable from the law, even though it is not clear;

3.5.1 Law

As discussed in section 1.4, the European regulator decided to make PbD mandatory for data controllers. Krebs highlighted the fact that there has been controversy among different stakeholders as to whether PbD should be codified into law.[271] In other words, the use of command and control mechanism through the means of legislation. For example, Koops criticizes the fact that even though the European

[265] Morgan B and Yeung K, *An introduction to law and regulation: Text and materials* (Cambridge University Press 2007).
[266] Morgan B and Yeung K, *An introduction to law and regulation: Text and materials* (Cambridge University Press 2007).
[267] Morgan B and Yeung K, *An introduction to law and regulation: Text and materials* (Cambridge University Press 2007).
[268] Morgan B and Yeung K, *An introduction to law and regulation: Text and materials* (Cambridge University Press 2007).
[269] Bennet, C and Raab, C, 'The Governance of Privacy: Privacy Instruments in global perspective' (2003), page 95.
[270] Klitou D, 'Privacy by design and privacy-invading technologies: Safeguarding privacy, liberty and security in the 21st century' (2011) 5(3) Legisprudence 297–329, page 324.
[271] Krebs D, "Privacy by Design': Nice-to-Have or a Necessary Principle of Data Protection Law?' (2013) Vol. 4, 2013 JIPITEC.

legislator has employed Code as a regulatory instrument by adopting a provision of PbD, it does so through means of a command-base law instead of a purely code approach.[272] Some industry players did concede that the approach taken by the regulator would be welcomed under the condition that there is no prescription of 'technological outcomes' or the use of certification schemes on that provision.[273]

In that regard, the Proposed Framework contains a criteria that advises that "Where resorting to law as a regulatory instrument, the standards should be 'clear, direct and understandable and their requirements should be realistic". From a design perspective, Schartum advanced that if the legislation facilitates the implementation of PbD, the approach's success would benefit and he suggested that pursuant to that, the legislation should be drafted with "distinctive characteristics of computers in mind".[274] However, Tsormpatzoudi et al find that the phrasing of the article is not necessarily easy and might compromise the implementation of the approach. [275] In fact, the factors present in Art.25 GDPR ("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") are arguably not easy to interpret, prioritize or to apply to specific contexts.

But there are other aspects to consider. As mentioned in 1.4, the Directive 95/46/EC[276] remained applicable throughout the emergence of new technologies because of its technology neutral concepts. Being that one aspect of the problem identified in 3.2 is the technological turbulence that is currently witnessed it is only logical that the GDPR should have the same attribute.[277] Furthermore, it has been acknowledged that a technology-specific approach to the legislation can be troublesome and that PbD is more adequate as a "general principle across all technologies."[278] The same reasoning was supported in the report "The Future of Privacy" and the alternative proposed there was that additional regulations should cover specific technological contexts with PbD provisions for those contexts.

In conclusion, while the current legislation text does not meet the criteria advanced above in the sense that it aids in the implementation of the approach (the requirement of clarity and understandable are not met), the co-regulation, consensus based approach put forth in the next sections has the ability to provide the clarity and support necessary that lack in the provision. This will be especially the case where other regulatory arrangements (communication/education through DPA regulation, WP29-like soft-law and etc.) will easily compensate for this. In my opinion in a more effective manner than trying to make the legislation technology-specific. Nevertheless, if solely judging the direction given by the regulator in the PbD

[272] Koops B, 'The trouble with European data protection law' (2014) 4(4) International Data Privacy Law accessed 20 December 2015 250–261.
[273] Krebs D, "Privacy by Design': Nice-to-Have or a Necessary Principle of Data Protection Law?' (2013) Vol. 4, 2013 JIPITEC, page 12.
[274] Wiese Schartum D, 'Making Privacy By Design Operative' (2016) 24 International Journal of Law and Information Technology, p.157.
[275] Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers (Springer 2016) 199–212.
[276] Directive 95/46/EC (Directive on protection of individuals with regard to the processing of personal data and on the free movement of such data).
[277] Working Party (WP) Article 29 D-95/46/EC.2009. The Future of Privacy. 02356/09/EN-WP 168.
[278] Krebs D, "Privacy by Design': Nice-to-Have or a Necessary Principle of Data Protection Law?' (2013) Vol. 4, 2013 JIPITEC, page 12.

provision of art. 25 GDPR, the command there is clear and understandable as it leaves no room for interpretation when it comes to the obligation to comply with the PbD approach.

3.5.2 Consensus and Self Regulation

Regulatory instruments based on consensus and co-operation are characterised by its voluntary nature. The certification mechanisms in GDPR's article 25 reads that *"*An approved certification mechanism (…) may be used (…) to demonstrate compliance with the requirements set out" (Data Protection by Design and Data Protection by Default). This is a form of consensus-based tool that the European Regulator incorporated, which couples the obligation (command and control) set out with consensus in order to modify behaviour. Thus, apart from giving direction and setting out the standards on a PbD obligation, the regulator decided to leverage a consensus instrument in order to assist the regulatees with compliance. On top of providing those data subjects as users of technology, products or services orientation in the marketplace, certification can also be relevant in relation to the data controllers' obligations under article 25.[279] Meaning that certification can assist the controller in demonstrating that it pursuant to fulfilling its PbD obligations, it considered PbD certified providers of technologies, products or services.

The use of consensus-based as a regulatory instrument is deductible from the above. To some extent is also possible to observe that decision in the normative design from other instances. Lachaud interpreted the regulators' decision of introducing certification as "an attempt to fill the gap existing between the traditional command and control regulation and the self-regulation instruments that flourished at the margin of the framework."[280]

As a matter of fact, through a Communication back in 2010 the EU regulator laid down two points: the purpose to explore self-regulatory initiatives such as Codes of Conduct; and to study the usefulness of "EU certification schemes in the field of privacy and data protection."[281] Recently, the WP29 emphasized the priority in providing guidance on the topic of certification as to prepare controllers and processors for entry into force of the GDPR.[282] Additionally, certification is not exclusive to the Data Protection by Design/Default provision, as it has been implemented in other sections of the Regulation for other aspects.

This option by the regulator is welcomed when assessed against the underlying framework. In fact, it is very much in line with the reasoning in 3.4.2, certification works as an incentive to regulatees, because organisations can use that certification to gain trust on the markets. In fact, Bock has recently stated that data protection certification is a positive incentive, one capable of creating market motivated changes in the

[279] European Commission, COM(2010) 609 final Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and The Committee of the Regions, *A comprehensive approach on personal data protection in the European Union*, Brussels, 4.11.2010.
[280] Lachaud E, 'Why The Certification Process Defined In The General Data Protection Regulation Cannot Be Successful' (2016) 32 Computer Law & Security Review, page 6.
[281] European Commission, COM(2010) 609 final Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and The Committee of the Regions, *A comprehensive approach on personal data protection in the European Union*, Brussels, 4.11.2010, page 13.
[282] Working Party (WP) Article 29 D-95/46/EC.2009. Statement on the 2016 action plan for the implementation of the GDPR 442/16/EN WP 236.

behaviour of organisations and the technology they create.[283] Basically, organisations can leverage certification as a mean to capitalize on data subjects trust and the competitive advantage that it entails (as discussed earlier). Thus, the choice of consensus through certification performs well agains the criteria of coherence between the Objectives been defined in line with regulatees interests.

Along the certification provisions, the GDPR, in its article 40 contains another regulatory instrument patent - self-regulation through Codes of Conduct. The article reads:

1. *The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.*

2. *Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to: (…)the measures and procedures referred to in Articles 24 and 25.*

Reading the paragraphs together it is possible to infer that private organisations representing data controllers (those obliged to comply with the PbD provision) can leverage this self-regulatory tool.

3.5.3 Code

Code as Law, as defined by Lessig[284] is an intrinsic part of PbD.[285] By leveraging the code approach, PbD is able to enforce technical rules embedded in architecture (e.g software). These rules, in the form of technical standards and protocols are able to ensure privacy in certain context like no other instruments. In fact, Klitou claims that without these technical means, regulations will be unable to ensure privacy by only leveraging law.[286] He further states, that only through the implementation of 'technological and design solutions' it will be possible to ensure compliance.[287] Indeed, over time the need for privacy enhancing technologies to be developed and employed in conjunction with legal, organizational, ethical and educational instruments has been advocated for.[288]

However, the criticisms to this regulatory instrument are plenty.[289] From an ethical and regulatory standpoint, code is criticized based on technological determinism and the restrictions on moral autonomy it may give rise to. However, these are not pointed to a specific form of regulation through code. Connecting the matter to PbD, regulators should not over-rely on the enforcement of privacy through code, because it

[283] Bock K, 'Data Protection Certification: Decorative Or Effective Instrument? Audit And Seals As A Way To Enforce Privacy' (Springer International Publishing Switzerland 2017).
[284] Lessig L, *Code: And other laws of Cyberspace* (3rd edn, Basic Books 1999).
[285] Klitou D, 'A Solution, But Not a Panacea for Defending Privacy: The Challenges, Criticism and Limitations of Privacy by Design' in Preneel, B and Ikonomou, D (Eds.) APF 2012, LNCS 8319, pp 86-110, 2014.
[286] Klitou D, 'Privacy by design and privacy-invading technologies: Safeguarding privacy, liberty and security in the 21st century' (2011) 5(3) Legisprudence 297–329, page 323.
[287] Klitou D, 'Privacy by design and privacy-invading technologies: Safeguarding privacy, liberty and security in the 21st century' (2011) 5(3) Legisprudence 297–329, page 323.
[288] Borking J and Raab C, 'Laws, PETs and Other Technologies for Privacy Protection', Refereed article, 2001 (1) The Journal of Information, Law and Technology (JILT). <http://elj.warwick.ac.uk/jilt/01-1/borking.html/>. New citation as at 1/1/04: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking/ .
[289] Gutwirth S, De Hert, P., De Sutter, L., 'The trouble with technological regulation from a legal perspective. Why Lessig's 'optimal mix' will not work.' (2008).

has limitations. Such limitations can be generally grouped in the business disincentives for 'code as code' and the difficulties in encoding legal rules.[290] One problem with code as regulation is that it can create the assumption that privacy (in a given context) is automatically achieved and create a misleading conviction that leads to individuals care less about their rights and make them more unware.

Koops highlighted the subjective nature of the PbD provision in the GDPR and pointed out that it can be interpreted in two ways. One entails organisations (data controllers) to deploy PETs, design-in privacy in practices, services and procedures and embed privacy safeguards as much as technically possible. The other entails "hard coding" privacy concepts and rules at code-level, which he deems to be impracticable, because it is not simple to code complex legal concepts in code.[291] He concludes that the former are preferable and that regulation should focus on creating a holistic privacy mind-set (as discussed in 3.4.2).[292] This opinion finds merit in the present thesis, because it goes hand-in-hand with the conclusions laid down so far. In this form, code can be fundamental in achieving privacy goals.

In conclusion, the normative choice to include a code aspect in the PbD provision of the GDPR is welcomed. However, it should be interpreted as the meaning above so as to no find defeat in technical impossibilities. Therefore, further steps should be for the regulator to create an environment where the development of those soft-coded measures and create business incentives for their adoption. In any case, either interpretation is deemed to be coherent. The use of Code as regulation is in line with the Problem as explained, the objective to shift the paradigm in privacy protection in way that will turn Privacy and Data Protection proactive and not reactive. This is because of code's automatic enforceability characteristic and the potential to code-in safeguards at design-level that will surely help privacy and data protection regulation to become proactive and no longer reactive.

3.5.4 Consideration of instruments and their optimal combination

From the previous sections, it is clear that the European regulator learned, in Brownsword's words, "the first lesson for smart regulators"[293] by understanding the problems of relying on single-instruments approach – solely judging from the GDPR it is possible to identify three different ones. Thus, the part of the criteria advanced in the Proposed Framework which mandates that regulators should consider the full range of available instruments is fulfilled. The focus is now on the part that suggests that regulators should strive for the deployment of optimal instrument mixes.

Reidenberg offered helpful insights into the optimal combination of instruments to govern privacy and data protection. First, he concluded that both law and technology (techno-regulation) cannot, on their own, provide effective regulation of privacy, because each has limitations.[294] By analysing the interdependence of law, self-regulation and code he also concluded that: *"*Law is necessary to establish the

[290] Koops B.-J, Bodea G, Hoepman J-H, Leenes R, Vedder A, D3.4 Code as Code Assessment (VIRTUOSO FP7 project (2009).Lessig L, *Code: And other laws of Cyberspace* (3rd edn, Basic Books 1999).
[291] Leenes R and Koops B, 'Privacy Regulation Cannot Be Hardcoded. A Critical Comment On The 'Privacy By Design' Provision In Data-Protection Law' (2013) 28 International Review of Law, Computers & Technology, page 160.
[292] Leenes R and Koops B, 'Privacy Regulation Cannot Be Hardcoded. A Critical Comment On The 'Privacy By Design' Provision In Data-Protection Law' (2013) 28 International Review of Law, Computers & Technology, page 160.
[293] Brownsword R, 'Code, Control, And Choice: Why East Is East And West Is West' (2005) 25 Legal Studies, page 2.
[294] Reidenberg, J, 'Privacy Protection and the interdependence of Law, Technology and Self-Regulation (2000).

public policy objectives, but insufficient to assure the implementation of fair information practices"[295] and that self-regulation falls short when it comes to assure the more humanistic aspect of privacy.[296] On the other hand, PbD in a form of code is believed to consist of an effective complement to regulatory and self-regulatory approaches.[297] Additionally, the OECD stated however that PbD (in form of PETs) must be deployed together with other instruments of educational or legislative nature. [298] Bennet and Raab also advance that in some cases PETs instead of complement can rather be an alternative to legislation.[299] As for certification, Easton states that in the past this regulatory tool has demonstrated faster outcomes than legal sanctions.[300] Additionally, she claims that when combined with legal sanctions, certification schemes prove to be more effective than self-regulation.[301] This was the approach taken by the European regulator.

Another modality to have into account is communication, which is, according to Tsormpatzoudi et al., required for the implementation of, for example, the Principle of PbD in light of EU Law.[302] It is advocated that teaching and training of all stakeholders is necessary to complement the provision that mandates PbD. Namely, in order to educate on the importance of PbD, the complexity of the concepts, the tools available to process data in a PbD compliant manner and more importantly, training on how to apply this knowledge in designing privacy into systems.[303] This reasoning fits one criteria left out of the Proposed Framework, but that is relevant in the present discussion – In Smart Regulation, one of the criteria advanced is to use motivational and informative instruments in order to best achieve the intended behaviour from the regulatees.[304]

In conclusion, the mix of policies employed by European regulator fits the optimal mix suggestions for privacy found in the literature. As we saw in 3.5 the regulator opted for law, consensus in a self-regulatory or co-regulatory fashion and code. The only instruments not identified and that were advocated for was instruments relying on the modality of communication. Thus, while the adoption of PbD in EU Law demonstrates effectiveness in its instrument choice, it shall be considered to follow the provision of the GDPR with tools of that nature – in that configuration the regulatory design is expected to benefit from it.

---

[295] Reidenberg, J, 'Privacy Protection and the interdependence of Law, Technology and Self-Regulation, page 10.
[296] Reidenberg, J, 'Privacy Protection and the interdependence of Law, Technology and Self-Regulation, page 4.
[297] Bennet, C and Raab, C, 'The Governance of Privacy: Privacy Instruments in global perspective' (2003), page 155.
[298] Organisation for Economic Co-operation and Development. Public Management Committee,OECD working papers: Reducing the risk of policy failure: challenges for regulatory compliance : 21st Session of the Public Management Committee, Château de la Muette, Paris 6-7 April 2000.
[299] Bennet, C and Raab, C, 'The Governance of Privacy: Privacy Instruments in global perspective' (2003), page 155.
[300] Easton C, 'Information Systems for Crisis Response and Management: The EU Data Protection Regulation, Privacy by Design and Certification' (Short Paper – Ethical, Legal and Social Issues Proceedings of the ISCRAM 2016 Conference – Rio de Janeiro, Brazil, May 2016 Tapia, Antunes, Bañuls, Moore and Porto de Albuquerque, eds.)
[301] Easton C, 'Information Systems for Crisis Response and Management: The EU Data Protection Regulation, Privacy by Design and Certification' (Short Paper – Ethical, Legal and Social Issues Proceedings of the ISCRAM 2016 Conference – Rio de Janeiro, Brazil, May 2016 Tapia, Antunes, Bañuls, Moore and Porto de Albuquerque, eds.)
[302] Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers(Springer 2016) 199–212;
[303] Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers(Springer 2016) 199–212;
[304] Grabosky P, Gunningham N and Sinclair D, *Smart Regulation: Designing Environmental Policy* (Oxford University Press 1998.

Against the criteria proposed, PbD not only fills the criteria of considering the full range of instruments, but also performed well in the optimal mix criteria.

3.6 Approach - Targets

One of the Problems identified in 3.2 is that law making in general, including Privacy and Data Protection laws around the globe, are reactive in nature. Law-like approaches that pursue Privacy objectives set their primordial goal at regulating the use of privacy invasive technologies in a reactive manner. The coherent response to this problem is the approach of PbD, which mandates that privacy and data protection are baked in the object that gives rise to risks – converting the reactive to proactive. It is only logic that Privacy by design be applied by the actual designers (producers, developers, etc.) of whatever the object in question.

From what can be gathered from the GDPR, the EU regulator took the regulatory approach to target data controllers, service providers and operators of IT systems.[305] Thus, they do not cover the application of the laws to developers or producers.[306] Klitou[307] argues that even though laws formulated as such (not covering producers) may indirectly influence producers to develop privacy compliant technologies, that it is not enough.

The situation that Klitou points out is that legislation is focusing on the users of privacy-intrusive technologies (data controllers, service providers, etc.), instead of focusing on their developers/manufacturers. He observes that the result is that the strategy of said legislation is to minimize the uncompliant use of those technologies, without addressing the intrusiveness of the technologies, which is the source of the problem.[308] As pointed out in section 3.2, this thesis subscribes to this reasoning. What Klitou is observing is a fundamental misalignment of the Problem and the targets (the Approach). Employing a logical and pragmatic reasoning, it seems as if Privacy by Design will not be truly effective, or at least, as effective as it could be if it does not cover the developers/producers of technologies that have a privacy-intrusive nature or that are not developed with data protection considerations.

The question of the producers/controllers that operate technologies or data processing systems is important. The PbD approach covers both and the EU regulator will miss an opportunity in case it does not frame the regulation as such. In fact, Rubinstein[309] arrives to the same conclusion to the applicability of the approach. He states that even though the design of products and data practices by organisations focus on two different aspects (which is line with the findings of this thesis in Chapter 1) of PbD, their objective is the same "to build in privacy protections using a combination of technological and organizational measures

[305] Klitou D, 'Privacy by design and privacy-invading technologies: Safeguarding privacy, liberty and security in the 21st century' (2011) 5(3) Legisprudence 297–329, page 298.
[306] Klitou D, 'Privacy by design and privacy-invading technologies: Safeguarding privacy, liberty and security in the 21st century' (2011) 5(3) Legisprudence 297–329, page 298.
[307] Klitou D, 'Privacy by design and privacy-invading technologies: Safeguarding privacy, liberty and security in the 21st century' (2011) 5(3) Legisprudence 297–329.
[308] Klitou D, 'Privacy by design and privacy-invading technologies: Safeguarding privacy, liberty and security in the 21st century' (2011) 5(3) Legisprudence 297–329.
[309] Rubinstein, Ira, Regulating Privacy by Design (May 10, 2011). Berkeley Technology Law Journal, Vol. 26, p. 1409, 2012. Available at SSRN: http://ssrn.com/abstract=1837862.

that ensure compliance with applicable rules"[310]. Thus, enforcing a PbD obligation solely on one of them is not coherent, unless otherwise addressed through other means.

In conclusion, there is lack of coherence between the Problem as explained, the objective to shift the paradigm in privacy protection in way that will turn Privacy and Data Protection proactive and not reactive.

[310] Rubinstein, Ira, Regulating Privacy by Design (May 10, 2011). Berkeley Technology Law Journal, Vol. 26, p. 1409, 2012. Available at SSRN: http://ssrn.com/abstract=1837862 , page 1425.

Conclusion

The objective of this thesis was to determine whether the incorporation of PbD in EU Law observes criteria of effective regulatory design.

Privacy by Design must be understood as an overarching concept that entails not only varied technological but also organisational aspects that aim for the enforcement of privacy and data protection principles in the context of the development of technologies, business practices and overall processes that carry processing of personal data or applications with privacy-invading potential.

Its concept, simply put, entails that privacy and data protection safeguards should be embedded in whatever relevant proposition (product, process, service, system, etc.) in the early stages of development as a default. That is the core meaning of PbD and something to be adopted by every stakeholder when dealing with such propositions and applying the principle.

Additionally, on a more high-level, it can be understood as an approach to tackle privacy and data protection from a regulatory point of view. Adopting a regulation pursuant to PbD entails recognizing and facilitating the use of technology as a regulatory instrument to pursue Privacy and Data Protection goals, the promulgation of legislation and promoting and prescribing the adoption of Privacy by Design way of tacking privacy matters.

The Problem that PbD seeks to address is the fact that Personal data is currently an important asset for business and governments, paired with the disruptive technological developments with privacy intrusive character that are systematically tackled in a way where technology is adapted to mitigate the problems after they come to light and when the damage is already done.[311] On top of that, those technologies are being developed and embraced at a pace that regulation cannot keep up with. The result is that regulation being lags behind, compromising the effective protection of privacy and data protection.

As for its Objectives, it was concluded for the need of the regulator to focus on the goal to pursue that data subjects are able to obtain control over their personal data and that businesses gain a competitive advantage while ensuring privacy. Additionally, one objective was proposed that was not so clearly identified by the legislator when interpreting the PbD provisions in the GDPR, is the shift of paradigm that reverts the reactive manner that has characterised the method through which EU Privacy and Data Protection policy can be characterised. Again, for the sake of coherence between the regulatory components and the approach, the regulators objectives must contain this rationale and it must be reflected in the rest of the regulatory design. Especially, in other regulatory efforts in the EU connected to PbD. This will render effectiveness.

With regards to the last and most crucial component of the regulatory design, the PbD approach itself, as explained in Chapter 1 proved to be the effective in face of the problem defined. The particular tuning in the choice of instruments was deemed effective in light of the Specific Criteria as the mix of policies employed by European regulator fits the optimal mix suggestions for privacy found in the literature. As we saw in 3.5 the regulator opted for law, consensus in a self-regulatory or co-regulatory fashion and

[311] Krebs D, "Privacy by Design': Nice-to-Have or a Necessary Principle of Data Protection Law?' (2013) Vol. 4, 2013 JIPITEC.

code. The only instruments not identified and that were advocated for was instruments relying on the modality of communication. Thus, while the adoption of PbD in EU Law demonstrates effectiveness in its instrument choice, it shall be considered to follow the provision of the GDPR with tools of that nature – in that configuration the regulatory design is expected to benefit from it. Thus, against the criteria proposed, PbD not only fills the criteria of considering the full range of instruments, but also performed well in the optimal mix criteria.

Furthermore, PbD as enshrined in the GPDR proved to be effective in the coherent choice of instruments. The use of Code as regulation is in line with the Problem as explained above and correspondent objective to shift the paradigm in privacy protection in a way that will turn Privacy and Data Protection proactive and not reactive. It is also in alignment with the objective to ensure individual's control over data and as for the general objective to ensure privacy. It is clear that the success of data protection and privacy are intimately connected to the success in the development of privacy techno regulation. Also, certification was found to be coherent with the objective to ensure organisations have a competitive advantage. The only instruments not identified in EU's PbD adoption, and that were advocated for, was instruments relying on the modality of communication. Thus, while the adoption of PbD in EU Law demonstrates effectiveness in its instrument choice, it shall be considered to follow the provision of the GDPR with tools of that nature – in that configuration the regulatory design is expected to benefit from it.

Finally, with regards to the choices of targets of the regulation, the major issue of ineffectiveness was raised as the approach and core reasoning of PbD was deemed to be incoherent with the definition of the targets. In fact, the regulators focus on the users of privacy-intrusive technologies (data controllers, service providers, etc.), instead of focusing on their developers/manufacturers. He observes that the result is that the strategy of said legislation is to minimize the uncompliant use of those technologies, without addressing the intrusiveness of the technologies, which is the source of the problem.[312]

The conclusion is that the major misalignment standing on the way of the effectiveness of the EU's adoption of PbD is the Problem and the actors that are targeted (the Approach). Employing a logical and pragmatic reasoning, it seems as if Privacy by Design will not be truly effective, or at least, as effective as it could be if it does not cover the developers/producers of technologies that have a privacy-intrusive nature or that are not developed with data protection considerations. Apart from that, the conclusion is that the regulatory intervention under assessment generally meets the criteria of effectiveness. The suggestions above are options to further improve that effectiveness.

[312] Klitou D, 'Privacy by design and privacy-invading technologies: Safeguarding privacy, liberty and security in the 21st century' (2011) 5(3) Legisprudence 297–329.

Bibliography

Primary sources:

- 'An Introduction To Data Protection' [2013] The EDRI Papers
- BUREAU OF CONSUMER PROTECTION, FED. TRADE COMM'N (FTC), PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2010).
- Business Dictionary, http://www.businessdictionary.com/definition/effectiveness.html accessed 28 November 2016.
- Cambridge Dictionary, 'Effectiveness meaning in the Cambridge English dictionary' (23 November 2016) <http://dictionary.cambridge.org/dictionary/english/effectiveness> accessed 28 November 2016.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
- Directive 95/46/EC (Directive on protection of individuals with regard to the processing of personal data and on the free movement of such data).
- DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)).
- European Commission, Communication from the commission to the European parliament and the council on promoting data protection by privacy enhancing technologies (PETs) COM/2007/0228 final (2007).
- European Commission, COM(2010) 609 final Communication from the Commission to the European Parliament, The Council, The Economic and Social Committee and The Committee of the Regions, *A comprehensive approach on personal data protection in the European Union*.
- European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, available at: http://www.refworld.org/docid/3ae6b3b70.html [accessed 3 June 2017]
- Information and Privacy Commissioner/Ontario, Landmark Resolution passed to preserve the Future of Privacy, http://www.ipc.on.ca/images/Resources/2010-10-29-Resolution-e_1.pdf
- Oxford Dictionaries, <https://en.oxforddictionaries.com/definition/effectiveness> accessed 19 September 2016.

- Privacy by Design Resolution at the 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem, 27 - 29 October 2010. Available online at
- http://www.privacyconference2011.org/htmls/adoptedResolutions/2010_Jerusalem/2010_J5.pdf
- 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, Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD).
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 10.1.2017 COM(2017) 10 final 2017/0003 (COD).
- 'Reducing The Risk Of Policy Failure: Challenges For Regulatory Compliance : 21St Session Of The Public Management Committee' [2000] OECD working papers
- Regulation (EU) 2016/679 of the European Parliament and of the Council 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.
- ULD (1996). Sommerakademie Datenschutz durch Technik – Technik im Dienste der Grundrechte. [Summer Academy Data Protection by Technology – Technology at the Service of Fundamental Rights.] https://www.datenschutzzentrum.de/sommerakademie/1996/sa96prog.htm; Summarised in a report available at https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/52DSK-KurzberichtZumDatenschutzDurchTechnik.pdf?blob=publicationFile
- Working Party (WP) Article 29 D-95/46/EC.2009. Statement on the 2016 action plan for the implementation of the GDPR 442/16/EN WP 236.
- Working Party (WP) Article 29 D-95/46/EC.2009. The Future of Privacy. 02356/09/EN-WP 168.

Secondary sources:

- Ayres I and Braithwaite J, Responsive Regulation (Oxford University Press 1992)
- Baldwin R, Cave M and Lodge M, 'Introduction: Regulation—The Field And The Developing Agenda' [2010] Oxford Handbooks Online
- Badiul Islam M and Iannella R, 'Privacy by Design: Does It Matter for Social Networks?' in Jan Camenisch and others (eds), Privacy and identity management for life: 7th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6 international Summer School, Trento, Italy, September 5-9, 2011, revised selected

papers (Springer-Verlag Berlin and Heidelberg GmbH & Co. K 2012) 207 – 220.Baldwin R, Rules And Government: Non-Statutory Rules And Administrative Law (Clarendon Press 1997)

- Bennet, C and Raab, C, 'The Governance of Privacy: Privacy Instruments in global perspective' (2003), page 196.
- Biegel S, Beyond Our Control? Confronting The Limits Of Our Legal System In The Age Of Cyberspace (MIT Press 2001)
- Black J, 'Critical Reflections On Regulation' Australian Journal of Legal Philosophy 27
- Black J, Rules And Regulators (Oxford University Press 1997)
- Blarkom G, Borking J and Olk J, Handbook Of Privacy And Privacy-Enhancing Technologies - The Case Of Intelligent Software Agents (ISBN 90 74087 33 7) (College bescherming persoonsgegevens 2003)
- Bock K, 'Data Protection Certification: Decorative Or Effective Instrument? Audit And Seals As A Way To Enforce Privacy' (Springer International Publishing Switzerland 2017)
- Borking J and Raab C, 'Laws, PETs and Other Technologies for Privacy Protection', Refereed article, 2001 (1) *The Journal of Information, Law and Technology (JILT)*. <http://elj.warwick.ac.uk/jilt/01-1/borking.html/>. New citation as at 1/1/04: <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking/>.
- Brennan D, 'The E-Privacy Regulation – What's New?'
    - http://www.algoodbody.com/insightspublications/the_eprivacy_regulation_whats_new accessed 12 June 2017
- Breyer S, Regulation And Its Reform (Harvard University Press 1984)
- Brownsword P and Goodwin M, Law And The Technologies Of The Twenty-First Century: Text And Materials (Cambridge University Press 2012)
- Brownsword R, 'Code, Control, And Choice: Why East Is East And West Is West' (2005) 25 Legal Studies
- Brownsword R, Rights, Regulation, And The Technological Revolution (Oxford University Press 2008)
- Brownsword, R. (2004), 'What the World Needs Now: Techno-Regulation, Human Rights and Human Dignity'. in: Global Governance and the Quest for Justice (edited by Brownsword, R.). 4: Human Rights. Hart, p. 203-234.
- Busch D and Levi-Faur A, , The regulation of privacy (Edward Elgar Publishing 2011)
- Cambridge Dictionary, 'Effectiveness Meaning In The Cambridge English Dictionary' (2016) <http://dictionary.cambridge.org/dictionary/english/effectiveness> accessed 28 November 2016

- Cavoukian A and Harbour P, 'Foreword By: Privacy By Design In Law, Policy And Practice' (2011) <https://www.ipc.on.ca/images/resources/pbd-law-policy.pdf> accessed 29 February 2016
- Cavoukian A, '7 Foundational Principles' (2009)
    - <https://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/> accessed 2 November 2015
- Cavoukian A, 'Privacy By Design In Law, Policy And Practice A White Paper For Regulators, Decision-Makers And Policy-Makers' <https://privacybydesign.ca/content/uploads/2011/08/pbd-law-policy.pdf> accessed 12 November 2015
- Cavoukian A, 'What Is Privacy By Design' (2009)
    - <www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf> accessed 2 November 2015
- Davies S, 'Why Privacy By Design Is The Next Crucial Step For Privacy Protection' <http://i-comp.org/wp-content/uploads/2013/07/privacy-by-design.pdf> accessed 14 October 2016
- De Hert P and others, Could the CE marking be relevant to enforce privacy by design in the Internet of things? (Springer Science + Business Media 2016)
- de Hert P, Poullet Y and Gutwirth S, Computers, Privacy And Data Protection: An Element Of Choice (Springer-Verlag New York 2011)
- Dix A, 'Built-In Privacy — No Panacea, But A Necessary Condition For Effective Privacy Protection' (2010) 3 Identity in the Information Society
- Dix A, “Betroffenenrechte im Datenschutz”, in Jan-Hinrik Schmidt and Thilo Weichert
    - (eds.), *Datenschutz, Bundeszentrale für politische Bildung*, (2012), pp. 290–297 [p. 296].
- Easton C, 'Information Systems For Crisis Response And Management: The EU Data Protection Regulation, Privacy By Design And Certification'
- ENISA, 'Privacy By Design In Big Data - Information Technology And Telecommunications - EU Bookshop' <http://dx.doi.org/10.2824/641480> accessed 15 October 2016
- Fukuyama F, Our Posthuman Future: Consequences Of The Biotechnology Revolution (Farrar, Straus and Giroux 2002)
- González Fuster G, 'Beyond The GDPR, Above The GDPR' [2015] Internet Policy Review <http://policyreview.info/articles/news/beyond-gdpr-above-gdpr/385> accessed 7 August 2016
- Grabosky P, Gunningham N and Sinclair D, Smart Regulation: Designing Environmental Policy (Oxford University Press 1998)
- Gurses S, Troncoso C and Diaz C, 'Engineering Privacy By Design', Conference on Computers, Privacy and Data Protection (CPDP 2011) (2011)

<https://lirias.kuleuven.be/bitstream/123456789/356725/1/article-1542.pdf> accessed 20 September 2016

- Hansen M, '‘Data Protection by Default in Identity-Related Applications’' in Simone Fischer-Hübner, Elisabeth de Leeuw, and Chris Mitchell (eds), Policies and Research in Identity Management: Third IFIP WG 11.6 Working Conference, IDMAN 2013 (2013).
- Hes, R., Borking, J.: Privacy Enhancing Technologies: the path to anonymity (Revised Edition) Registratiekamer, Achtergrondstudies en Verkenningen 11 (first edition 1995);
- Hoepman J-H, Hansen M, and Jensen M, 'Towards measuring maturity of privacy-enhancing technologies' in Bettina Berendt and others (eds), Privacy Technologies and Policy - Third Annual Privacy Forum, APF 2015 Luxembourg, Luxembourg, October 7 – 8, 2015 Revised Selected Papers (Springer Science + Business Media 2016) 3 – 20.
- Holland D and Quinn N, 'Culture And Cognition', Cultural Models in Language and Thought (Cambridge University Press 1987)
- Hustinx P, 'Privacy By Design: Delivering The Promises' (2010) 3 Identity in the Information Society <http://dx.doi.org/10.1007/s12394-010-0061-z> accessed 25 February 2016
- Ikonomou D and others, , Designing Privacy-by-Design (2014)
- Ikonomou D and others, , Privacy-ABCs as a case for studying the adoption of pETs by users and service providers (Springer Science + Business Media 2016)
- Information and Privacy Commissioner/Ontario, *Privacy-enhancing technologies: The path to anonymity* (John J. Borking and Ronald Hes eds, Registratiekamer 1995).
- Jenkins W I, Policy Analysis: A Political and Organizational Perspective (St Martin's Press, 1978) 15
- Kindt E, Privacy And Data Protection Issues Of Biometric Applications (Springer Netherlands 2013)
- Klitou D, 'Privacy By Design And Privacy-Invading Technologies: Safeguarding Privacy, Liberty And Security In The 21St Century' (2011) 5 Legisprudence
- Klitou D, Privacy-Invading Technologies And Privacy By Design: Safeguarding Privacy, Liberty And (Springer 2014)
- Koops B.-J, Bodea G, Hoepman J-H, Leenes R, Vedder A, D3.4 Code as Code Assessment (VIRTUOSO FP7 project (2009)
- Krebs D, 'Privacy By Design': Nice-To-Have Or A Necessary Principle Of Data Protection Law?' (2013) Vol. 4, 2013 JIPITEC

- Lachaud E, 'Could the CE marking be relevant to enforce privacy by design in the Internet of things?' in Serge Gutwirth, Ronald Leenes, and Paul De Hert (eds), Data Protection on the Move - Current Developments in ICT and privacy/Data Protection (Springer Science + Business Media 2016) 135–162
- Lachaud E, 'Why The Certification Process Defined In The General Data Protection Regulation Cannot Be Successful' (2016) 32 Computer Law & Security Review
- Le Métayer D, 'Privacy By Design: A Matter Of Choice' [2010] Data Protection in a Profiled World
- Leenes R and Koops B, 'Privacy Regulation Cannot Be Hardcoded. A Critical Comment On The 'Privacy By Design' Provision In Data-Protection Law' (2013) 28 International Review of Law, Computers & Technology
- Leenes R and Koops B, 'The Trouble With European Data Protection Law' (2014) 4 International Data Privacy Law
- Leenes R and others, , On the Principle of Privacy by Design and itsLimits: Technology, Ethics and the Rule of Law (Springer Science & Business Media 2012) <https://books.google.nl/books?id=xucZva6XhPQC&pg=PA343&dq=aims+of+privacy+by+design&hl=en&sa=X&ved=0ahUKEwjNivruyqLLAhWBPg8KHeRkAw0Q6AEINjAE#v=onepage&q=aims%20of%20privacy%20by%20design&f=false> accessed 2 March 2016
- Leenes R, de Hert P and Gutwirth S, European Data Protection: In Good Health? (Springer 2012)
- Lessig L, Code: And Other Laws Of Cyberspace (3rd edn, Basic Books 1999)
- Levi-Faur D and Braithwaite J, Regulatory Capitalism: How It Works, Ideas For Making It Work Better (Elgar, Edward Publishing 2008)
- Lodge M, Baldwin R and Cave M, The Oxford Handbook Of Regulation (Oxford Handbooks In Business & Management) (Oxford University Press, USA 2010)
- Lodge M, Cave M and Baldwin R, Understanding Regulation: Theory, Strategy, And Practice (2nd edn, Oxford University Press 2012)
- Mitchell C and others, ‘Data Protection by Default in Identity-Related Applications (2013)
- Noll R and Selznick P, , Focusing Organizational Research of Regulation (1985)
- Ogus A, Regulation: Legal Form And Economic Theory (Clarendon Law Series) (Clarendon Press 1994)
- Olk J, Borking J and Blarkom G, Handbook Of Privacy And Privacy-Enhancing Technologies - The Case Of Intelligent Soft- Ware Agents (College bescherming persoonsgegevens 2003)

- Pagallo U, 'On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law' in Serge Gutwirth and others (eds), *European data protection: In good health?* (Springer Science & Business Media 2012) 342.
- Pedreschi D and others, 'Privacy-By-Design In Big Data Analytics And Social Mining' (2014) 3 EPJ Data Science
- 'Privacy By Design Strong Privacy Protection – Now, And Well Into The Future A Report On The State Of Pbd To The 33 Rd International Conference Of Data Protection And Privacy Commissioners' (Ontario Information & Privacy Commissioner 2012) <https://www.ipc.on.ca/images/Resources/PbDReport.pdf> accessed 29 February 2016
- Reidenberg, J, ‘Privacy Protection and the interdependence of Law, Technology and Self-Regulation (2000).
- van Rest J and others, 'Designing Privacy-by-Design' in B Preneel and D Ikonomou (eds), Privacy Technologies and Policy - First Annual Privacy Forum, APF 2012 Limassol, Cyprus, October 2012 Revised Selected Papers(2014).
- Rubinstein I, 'Regulating Privacy By Design' (2011) Vol.26 Berkeley Technology Law Journal
- Russello G and others, , Privacy by Design: Does It Matter for Social Networks? (Springer-Verlag Berlin and Heidelberg GmbH & Co K 2012)
- Schaar P, 'Privacy By Design' (2010) 3 Identity in the Information Society
- Schellekens M and others, Starting Points For ICT Regulation: Volume 9: Deconstructing Prevalent Policy One-Liners: V. 9 (TMC Asser Press 2006)
- Schiffner S and others, , Towards measuring maturity of privacy-enhancing technologies (Springer Science + Business Media 2016)
- Schiffner S and others, , Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity (Springer 2016)
- Scott C, Hood C and Baldwin R, A Reader On Regulation (Oxford University Press 1998)
- Sheehy B and Feaver D, 'Designing Effective Regulation: A Normative Theory' (2015) 38 University of New South Wales Law Journal.
- Solove D, Understanding Privacy (Harvard University Press 2008)
- Spiekermann, S, The challenges of privacy by design. Commun. ACM 55(7)(2012), 38-40.
- Tsormpatzoudi P, Berendt B, and Coudert F, 'Privacy by Design: From research and policy to practice - the challenge of multi-disciplinarity' in Bettina Berendt and others (eds), Privacy technologies and policy: Third annual privacy forum, APF 2015, Luxembourg, Luxembourg, October 7-8, 2015, revised selected papers (Springer 2016) 199–212.

- Tsormpatzoudi P, Coudert F, PRIPARE, Deliverable D5.1 State-of-Play: Current Practices and Solutions (2014) http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE_Deliverable_D5.1_v1.0.pdf
- van den Berg B, 'Mind The Air Gap' [2016] Law, Governance and Technology Series
- Verheyen K, Arts B and Van Gossum P, 'From "Smart Regulation" To "Regulatory Arrangements"' (2010) 43 Policy Sciences
- Vibert F, The New Regulatory Space: Reframing Democratic Governance (Edward Elgar Publishing 2014)
- Viola de Azevedo Cunha M, Market Integration Through Data Protection: An Analysis Of The Insurance And Financial Industries In The EU (Springer 2013)
- Wiese Schartum D, 'Making Privacy By Design Operative' (2016) 24 International Journal of Law and Information Technology
- Yeung K and Morgan B, An Introduction To Law And Regulation: Text And Materials (Cambridge University Press 2007)